2002-06

Research in computer forensics

Wai, Hor Cheong

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

RESEARCH IN COMPUTER FORENSICS

by

Hor Cheong Wai

June 2002

Thesis Co-Advisors: Daniel F. Warren
Dan C. Boger

Approved for public release; distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2002	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Research in Computer Forensics			**5. FUNDING NUMBERS**
6. AUTHOR(S) Hor Cheong Wai			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT

Computer Forensics involves the preservation, identification, extraction and documentation of computer evidence stored in the form of magnetically encoded information. With the proliferation of E-commerce initiatives and the increasing criminal activities on the web, this area of study is catching on in the IT industry and among the law enforcement agencies.

The objective of the study is to explore the techniques of computer forensics from the computer security perspective. Specifically, the thesis looks into the application of forensic principles and techniques, security designs of computer hardware and software, and network protocols, in an effort to discover the trails of the computer hackers. The thesis subsequently packages this knowledge into a curriculum for a twelve weeks resident course at the Naval Postgraduate School.

Complementing the research and course materials are surveys conducted on agencies and vendors currently providing computer forensic courses and training, reading materials, and software tools applicable to computer forensic investigation. The purpose of these surveys is to provide a depository of useful information related to this specialized discipline of computer security.

It is the hope of the study that students in the future will benefit from the knowledge gathered in this thesis and the exposure gained from the course and laboratory exercises will allow them to correctly respond to computer intrusions and unauthorized activities they may encounter on their C4I systems.

14. SUBJECT TERMS Computer Forensics, Cyber Crime Investigation, Computer Security			**15. NUMBER OF PAGES** 205
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

RESEARCH IN COMPUTER FORENSICS

Hor Cheong Wai
Major, Republic of Singapore Navy
B.S., National University of Singapore, 1993

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
June 2002

Author: Hor Cheong Wai

Approved by: Daniel F. Warren, Thesis Co-Advisor

Dan C. Boger, Thesis Co-Advisor

Dan C. Boger, Chairman
Information Systems Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Computer Forensics involves the preservation, identification, extraction and documentation of computer evidence stored in the form of magnetically encoded information. With the proliferation of E-commerce initiatives and the increasing criminal activities on the web, this area of study is catching on in the IT industry and among the law enforcement agencies.

The objective of the study is to explore the techniques of computer forensics from the computer security perspective. Specifically, the thesis looks into the application of forensic principles and techniques, security designs of computer hardware and software, and network protocols, in an effort to discover the trails of the computer hackers. The thesis subsequently packages this knowledge into a curriculum for a twelve weeks resident course at the Naval Postgraduate School.

Complementing the course materials are surveys conducted on agencies and vendors currently providing computer forensic courses and training, reading materials, and software tools applicable to computer forensic investigation. The purpose of these surveys is to provide a depository of useful information related to this specialized discipline of computer security.

It is the hope of the study that students in the future will benefit from the knowledge gathered in this thesis and the exposure gained from the course and laboratory exercises will allow them to correctly respond to computer intrusions and unauthorized activities they may encounter on their C4I systems.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

DESCRIPTION OF THE THESIS 1
A. INTRODUCTION 1
B. COMPUTER SECURITY EDUCATION IN NPS 2
C. WHY A COMPUTER FORENSIC COURSE IN NPS 3
D. WHAT IS COMPUTER FORENSICS 6
E. SURVEY OF AGENCIES AND VENDORS PROVIDING COMPUTER FORENSIC COURSES AND TRAINING 6
F. SURVEY OF READINGS ON COMPUTER FORENSIC 7
G. SURVEY OF TOOLS FOR COMPUTER FORENSIC INVESTIGATION 7
H. DESCRIPTION OF THE COMPUTER FORENSIC COURSE 8
I. MATERIALS FOR COURSE LECTURES 9
J. CONTENTS OF THE COURSE 10
1. Cyber Crime & Incident Response 10
2. Introduction to Computer Forensics 10
3. Application of Forensic Science to Computers 11
4. Structure for Forensic Investigations 11
5. Computer Forensic Procedures 11
6. Forensics using MAC Times 11
7. Forensics on Windows 12
8. Forensics on Unix 12
9. Forensics on the Networks 12
10. Forensics on an Unknown Program 13
11. Forensics on Intrusion Activities 13
12. Forensics on Wireless Network 13
K. LABORATORY EXERCISES 14
L. SUMMARY OF THE LABORATORY EXERCISES 14
1. Foundstone Forensic Toolkit 14
3. AccessData Forensic Toolkit 15
4. Windows Event Log Analysis 15
5. DumpEvt (SomarSoft) 16
6. Unix Log Analysis 16
7. Network Analysis 17
M. CONCLUSION 18

APPENDIX A: LIST OF AGENCIES AND VENDORS PROVIDING COMPUTER FORENSIC COURSES AND TRAINING 19

APPENDIX B: LIST OF READINGS ON COMPUTER FORENSICS 33

APPENDIX C: LIST OF TOOLS FOR COMPUTER FORENSIC INVESTIGATION 45

APPENDIX D: SUMMARY OF REQUIREMENTS OF A COMPUTER FORENSIC INVESTIGATOR 57

APPENDIX E: HANDOUTS FOR COURSE LECTURES 61

APPENDIX F: HANDOUTS FOR LABORATORY EXERCISES 173

LIST OF REFERENCES 191

INITIAL DISTRIBUTION LIST 193

ACKNOWLEDGMENTS

I would like to thank Senior Lecturer Daniel F. Warren and Professor Dan C. Boger who shared their time and knowledge in helping me complete this thesis. Specifically, I would like to thank them for their enthusiastic guidance, tutelage, and patience towards the completion of the research.

I would also like to thank Hardware Support Technician Michael Williams from the Computer Science Department, and Research Associate David Riebandt from the Center for Information Assurance and INFOSEC Studies and Research, in helping me resolve some of the hardware and software glitches I have encountered while setting up the network environment for the laboratory exercises.

Finally my sincerest appreciation, gratitude and admiration go to my lovely wife Mei Leng, a defense software engineer by training, who has given me invaluable technical assistance in developing the laboratory exercises and her patience, love and understanding during the course of this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

DESCRIPTION OF THE THESIS

A. INTRODUCTION

The objective of the study is to explore the techniques of computer forensics from the computer security perspective and package this knowledge into a curriculum for a twelve week resident course at the Naval Postgraduate School (NPS). Specifically, the thesis has looked into the application of forensic principles and techniques, security designs of computer hardware and software, and network protocols, in an effort to discover the trails of the computer hackers.

This course is intended to provide students with an understanding of the fundamentals of computer forensics. Students will examine how information is stored in computer systems and how it may be deliberately hidden and subverted. The course will establish a sound theoretical foundation on the methods used in extracting information for evidential purposes before going on to emphasis practical forensic examination and analysis. It will also cover the techniques of computer evidence recovery and the successful presentation of such evidence before the court.

Complementing the course materials are surveys conducted on agencies and vendors currently providing computer forensic courses and training, reading materials, and software tools applicable to computer forensic investigation.

While it is not the purpose of this course to train students to become computer forensic experts within such a brief period of instruction, it is hoped that it can provide basic computer forensic knowledge to the Computer Science and Information Technology graduates. If more students from NPS become experienced in the fundamentals of computer forensics, then more Military Commands will be able to benefit from the capability of these graduates to correctly respond to computer intrusions and unauthorized activities on their C4I systems.

B. COMPUTER SECURITY EDUCATION IN NPS

Educating students in the techniques of computer and network security demands an institution that is properly equipped with the necessary resources in order to stay current with both information system technology and advances in computer security threat, tools, techniques, solutions and risk containment. Students aspiring to become Information Security (INFOSEC) professionals must receive the relevant education and good training foundations to work effectively in a variety of INFOSEC situations. Since the underlying technologies are changing so rapidly, yesterday's most significant problem and solution may be of no relevance tomorrow. As such, they need to be educated broadly enough to allow them to move rapidly to new problem areas and new technologies.

During the "Goals for Computer Security Education" forum at NPS, Jim Schindler, a participant from HP, mentioned that technology is changing, computer paradigms are changing, and security requirements are changing. He considered security education a must for a much larger community than security professionals. [6] The explosive growth of information systems has resulted in rapidly changing technologies and challenges in computer security. Continued curriculum development is necessary to ensure a timely, coherent and comprehensive program in INFOSEC foundations and technology.

NPS has fostered an academic environment to examine the INFOSEC requirements of the Department of Defense (DoD) and address the challenges presented by those requirements. It has developed a strong curriculum for computer and network security courses and continues to conduct leading-edge research in problems related to information assurance. These initiatives not only increase an appreciation of the foundations of computer security, but also heighten an understanding of the need to consider security throughout the entire process of system design and development. Through the Center for Information Assurance and INFOSEC Studies and Research (CISR), NPS has been producing a talent pool of computer security savvy graduates to apply to the variety of INFOSEC challenges in the DoD. [7]

C. WHY A COMPUTER FORENSIC COURSE IN NPS

Computer and network security is not a discipline for the isolationist. Computer security education needs to produce individuals who have a broad understanding of the scope of the discipline as well as considerable knowledge and expertise in specific areas. [8] Computer forensics, the application of established forensic methodology in the examination of computer crime, is one of these specific areas that have gained increasing emphasis in large corporations and especially in the defense organizations. No longer are organizations content with relying solely on national Computer Emergency and Response Teams (CERT) or law enforcement agencies to perform investigation on suspected compromise in their computer systems. More and more of them are gearing up to arm themselves with in-house computer forensic skills to meet the increasing likelihood of threats to their "corporate lifelines". Many organizations' business functions will come to a halt if their network computer system collapses. No longer are they willing to rely solely on the advice of the CERT organizations or law enforcement agencies who are likely to shut off their entire system even if the suspected security compromise is only reported in a localized sector of the network.

This developing trend is a result of numerous motivations. Given the volatile nature of digital information in the computer and magnetic media, digital evidence in the system can be potentially destroyed when one responds to a suspected intrusion, whether by "doing something or doing nothing". As most computer security professionals will advocate, having an incident response plan is not just fashionable. From the instance an intrusion is detected, every additional action taken, whether trivial or not, can bring considerable consequence to the success of an investigation effort. Even having a thoroughly tested incident response plan is not fool-proofed. Responding to reported computer security incidents require constant evaluation of the effects observed so far, before taking the next step. However, if one is armed with basic knowledge in computer forensics, then one is more likely to be able to accurately anticipate the consequential effects. The likelihood of success that each action taken to contain the damage to the system and towards the investigation effort can also be dramatically improved. Arming computer security professionals within the organization with basic computer forensic skills can enable the organization to react correctly in the first few moments of a reported

computer security incident by facilitating the preservation of digital evidence for the subsequent investigation when the "big boys" or experts takeover the case.

Due to increasingly confusing business client privacy legislation and the liability that an organization faces if its computer system has been used as a tool to attack another computer system, many organizations are finding it more attractive to conduct their own computer security incident investigations than report them to the authorities, unless they have already developed into an advanced stage that can no longer be hidden from the general public's notice. Whenever feasible, organizations will prefer not to alarm their clients or risk their reputation by announcing or admitting the existence of a computer security incident. Not only will this blemish an organization's standing in the industry and market competitiveness, it may also bring on the unwelcomed involvement of law enforcement agencies and media attention. Once an investigation has escalated to the point of law enforcement agency involvement, the confidentiality of the organization's sensitive information on its clients, market strategy, competitive advantage initiatives and "dirty laundry" comes under the mercy of the external investigators. Thus, harnessing basic computer forensic skills in-house will enable organizations to conduct their own investigations and keep the incident within its own perimeter, especially for minor incidents that can be conveniently "swept under the carpet".

If an organization is an agency in a defense department, the argument for in-house computer forensic expertise is even greater. In this case, an alarm may not just cause a loss of public confidence, but also public panic, because DoD's information is so pertinent to national security interests. Thus, it is not surprising that ministries, military establishments, and the state and defense departments all have their own computer forensic expertise in varying degrees. Since technology is the most effective force multiplier in modern combat, most defense and military organizations have invested heavily on C4I in their force structure. As such, computer technology, information protection and networking have become indispensable in the military infrastructure with military systems becoming increasingly dependent upon the national information infrastructure for critical services. A key aspect of achieving and maintaining information superiority is the protection of critical national information assets. In fact, "cyberwar"—creating havoc in the national information infrastructure of an adversary—has been

identified by many armed forces as one of the important strategic options. Many defense organizations have placed considerable emphasis on safeguarding their C4I systems and mastering techniques to deny the enemy effective use of their C4I system. The detection of an initial computer attack could be an early warning sign of an impending military attack because, as is common in many military options, the first strike leading to the escalation to a full-blown war is generally an operative that will bring an asymmetric effect to the enemy and least risk of casualties to their own force. However, it is important for the military to be able to promptly distinguish between attacks carried out by "script kiddies" from the orchestrated attacks sponsored by state players. To this effect, defense organizations have, in tandem to their civilian law enforcement counterparts, developed advanced technologies in the discipline of computer forensics. Unfortunately, the opportunities for computer forensic training in defense organizations have been limited generally to individuals and agencies that are highly specialized in the area. Even though increasing numbers of subordinate Commands are developing and operating their own computer systems, most do not have any computer forensic considerations beyond their standard incident response plans. Thus, as with business corporations, it is becoming increasingly attractive for individual Military Commands to possess a sufficiently high level of computer forensics capabilities.

To date, only the Royal Military College of Science (RMCS), United Kingdom, has a program leading to a Postgraduate Diploma or Master of Science in Forensic Computing. Thus it is imperative that NPS consider developing such a curriculum when the resources become available. As a start, it can provide basic computer forensic knowledge to the Computer Science and Information Technology graduates. If more students from NPS become experienced in the fundamentals of computer forensics, then more Military Commands will be able to correctly respond to detected computer intrusions and unauthorized activities on their C4I systems. It is this motivation that has lead to the formulation of computer forensic material for a potential Computer Forensic Course at NPS.

D. WHAT IS COMPUTER FORENSICS

Computer forensics involves the preservation, identification, extraction, analysis, documentation and presentation of computer evidence. This computer evidence is useful in criminal cases, civil disputes, and human resources/employment proceedings. Many times computer evidence is created transparently by a computer's operating system and without the knowledge of the computer user. Such information is often hidden from view so that special forensic software tools and techniques are required to preserve, identify, extract and document it. It is frequently this information that benefits law enforcement and military agencies the most while gathering evidence during an investigation.

With the proliferation of computers in the workplace, it should be no surprise that computer technology is involved in a growing number of crimes. As more criminals use technology to achieve their goals and avoid apprehension, there is a developing need for specialists who can analyze and use digital evidence stored on and transmitted by computers. [2] As such, the discipline of computer forensic analysis has emerged to meet such needs. Computers can contain evidence in many ways, in electronic mail systems, on network servers and on individual's computers. However, due to the ease with which computer data can be manipulated, the search and analysis need to be performed by a trained computer forensic specialist, otherwise it will likely lead to evidence being either overlooked or rendered legally useless.

E. SURVEY OF AGENCIES AND VENDORS PROVIDING COMPUTER FORENSIC COURSES AND TRAINING

The field of computer forensic investigation is a relatively new addition to the forensic sciences. Computer forensic analysis requires a thorough and painstaking examination of digital evidence. This evidence may take the form of digitally stored documents, photographs, sounds, motion pictures, spreadsheets, databases, Internet history files, or any other recording in digital form. In addition, the examiner may be asked to retrieve these documents or recordings after they have been deleted, fragmented or encrypted. This mandates that the forensic examiner have a diverse set of both technical and investigative skills. Due to the exponential growth of computer technology

and the increasing rate of change in that technology, law enforcement and government agencies are unable to continually provide qualified computer forensic examiners. When the area of computer forensics was established more than a decade ago, there was no standard as to what comprises a basic or advanced computer forensic training, education or certification program. [9] Since then, there have been numerous activities and efforts by the industry and computer security agencies to define the concepts and structures of computer forensics. Currently, training in computer forensics is widely available. It is offered by government, private and academic organizations, with some programs are only available for law enforcement officers. A list of the agencies and vendors providing computer forensic courses and training is detailed in Appendix A. These may prove to be valuable sources for maintaining staff expertise and course currency in the future.

F. SURVEY OF READINGS ON COMPUTER FORENSIC

The number of published books, journals and articles related to computer forensics has blossomed dramatically in recent years. Many of these books and publications are written within the last three years. In addition, many credible sources of information related to computer forensics can be found on the websites of numerous interest groups, INFOSEC agencies, law enforcement organizations and vendors providing computer security solutions. While it is not possible to read and comment all of these materials, a list of books on computer forensics has been provided in Appendix B with brief editorial reviews and selected readers' comments. It is hoped that this list will facilitate the lecturer and student who is interested in reading material that is beyond the scope of the course.

G. SURVEY OF TOOLS FOR COMPUTER FORENSIC INVESTIGATION

The use of computer forensics tools is invaluable in gathering computer forensics information. Computer forensic software tools can be used to identify passwords, backdated files, network logins, files stored in a computers memory and the hard disk; and associate an external document to a specific computer. A list of popular computer forensics toolkits is consolidated in Appendix C. Due to relatively limited demands for

such specialized toolkits, most of these computer forensic suites are not widely advertised or promoted.

Examining a computer for forensic evidence generally requires another computer and a set of forensics tools. Various developers and vendors of computer forensic analysis software have their own unique perspective on the needs of the investigative community and their own approach as to how to meet those needs. An investigator would naturally desire a forensic analysis toolbox to have all possible forensic capabilities. However, in reality, there is no such a universal toolbox. What the various developers and vendors have produced is a suite of tools that meets a significant majority of an investigator's needs. James Holley's Meeting Computer Forensic Analysis Requirements [5], which are summarized in Appendix D, provides an overview of such requirements.

H. DESCRIPTION OF THE COMPUTER FORENSIC COURSE

This course is intended to provide students with an understanding of the fundamentals of computer forensics. Students will examine how information is stored in computer systems and how it may be deliberately hidden and subverted. The course will establish a sound theoretical foundation on the methods used in extracting information for evidential purposes before going on to emphasis practical forensic examination and analysis. It will also cover the techniques of computer evidence recovery and the successful presentation of such evidence before the court.

Laboratory facilities will be used to introduce students to the use of common computer forensic tools, the principle of original integrity, disk examination, logging and preparation of evidence. Further descriptions of the laboratory exercises are found in the section on Laboratory Setup and Instruction Manual.

Recommended prerequisites for the Computer Forensic Course shall ideally include the incumbent CS3600—Introduction to Computer Security and CS3670—Secure Management of Systems. These computer security foundation courses will provide students with a good understanding of the security mechanisms that are in place in most computer systems and how they can aid in the recovery of digital evidence in a forensic analysis. Exposures to hacking techniques and tools in CS3675—Internet

Security Resources and Policy, will further enhance the students' appreciation on the characteristics of genetic tracks left behind by these security exploits. However, this course is not an absolute prerequisite.

Based on the scope and magnitude of the course materials, weekly instruction with three hours of lectures and two hours of laboratory exercises should be adequate for the students to complete the syllabus at a comfortable pace, with opportunities to clarify doubts during classes and considering the occasional cancellation of classes on official holidays within an academic quarter.

I. MATERIALS FOR COURSE LECTURES

The course materials were gathered from various books, journals and on-line articles. In order to support a course that provides wide coverage of many relevant topics, much of the content is derived from the main sources described below.

Materials on the application of forensic methodology in a computer crime investigation were extracted from *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* by Eoghan Casey. [2] The *Handbook of Computer Crime Investigation: Forensic Tools & Technology*, which is edited by Eoghan Casey [3] consists of chapters written by a few top experts, provided materials for the three aspects of the course. It provided a good description of some of the leading computer forensic tools, simple to read technical information for collecting and analyzing digital evidence, and case examples of the technical, legal and practical challenges in real computer investigations.

The on-line Computer Forensics Column from the Doctor Dobb's Journal column by Dan Farmer and Wietse Venema [4] provided good technical coverage on forensic techniques for the Unix and Linux environment. Some of the materials were also borrowed from the Unix Computer Forensics Analysis Class that was conducted at the IBM Thomas J Watson Research Center in August 1999. These on-line materials are free and available on either *www.fish.com/security/ddj.html* or *www.porcupine.org/forensics*.

Last but not least, The Process of Network Security: Design and Managing a Safe Network by Thomas Wadlow [10] helped to fill in the management perspectives on responding to computer-related incidents and advice on how to facilitate the activities of a computer forensic investigation.

While a course text is not absolutely necessary, the Handbook of Computer Crime Investigation: Forensic Tools & Technology, by Eoghan Casey, is a recommended reference text. Students who are unfamiliar with Unix or Linux can refer to the on-line Computer Forensics Column from the Doctor Dobb's Journal column series by Dan Farmer and Wietse Venema.

J. CONTENTS OF THE COURSE

The course content is organized into the following twelve sections, each covering a specific area related to the topic.

1. Cyber Crime & Incident Response

This section starts with an explanation on how computers and networks could be used as instruments for crime, the types of cyber crimes and computer crime prosecution. Incident response is described in terms of the necessary reaction measures, procedural steps and priorities, investigation checklist and risk management.

2. Introduction to Computer Forensics

This introduction to computer forensics focuses on the collection and use of digital evidence, hardware, information media and physical evidence. It also describes the controversies of whether to turn the computer off or leave it running when an attack is detected and on reporting the computer crime to the law enforcement agencies.

3. Application of Forensic Science to Computers

Computer forensics applies the basic principles of forensic science to computer crime investigation. It describes the fundamentals and highlights issues pertaining to the recognition, preservation, collection, documentation, classification, comparison, individualization and reconstruction of the digital evidence.

4. Structure for Forensic Investigations

The structural requirements for forensic investigations emphasizes the importance of preserving the integrity of the digital evidence by first testing the reliability of the forensic tools used for formulating the leads in the investigations. It also highlights some of the specific issues related to data and evidence recovery. The last part of this section describes ways to characterize an intrusion and how an examiner's mindset can influence the success of the investigation.

5. Computer Forensic Procedures

This section steps through the common computer forensic procedures in details. It differentiates the differences between physical from logical examinations. It also highlights the challenges of investigating criminal activities, problems of gaining access to the relevant data, opportunities for tampering and the chain of trust. Understanding the data storage and its logical abstraction are necessary for preparing, imaging, processing, filtering, preserving and reconstructing the evidentiary images. Thereafter, the digital evidence shall be indexed and bates numbered for electronic management and future reference.

6. Forensics using MAC Times

MAC Times represent the last time a file was modified, accessed or had its attributed changed. The analysis of the MAC Times has often been invaluable in helping the examiner understand how files in the system were manipulated or

deleted during the crime. The section also cautions how the MAC Times could be subjected to tampering.

7. Forensics on Windows

This section starts with an introduction of the Windows master file table and metafiles for the NT file system and the folder entries for the file allocation table. It goes on to describe the characteristics of the recycle bin, shortcut files, registry entries, printer spool and operating system logs for the system events, internet information server, Exchange mail server, Outlook mail client and Active Directory; and how digital evidence can be recovered from these information depositories.

8. Forensics on Unix

Similar to the previous section, this section starts with an introduction of the user permissions, shared files and system services. The numerous standard logs and the Shell history files in the Unix operating system commonly provide a rich source of digital evidence. The section also describes the process of restoring information from backup tapes and on duplicating the hard drive. It notes that some of the system events are not necessarily recorded in the system logs and how entries in these logs can be manipulated or tampered. Understanding the details of the Unix file system, the file attributes, and their logical and physical properties, is necessary to comprehend the effects of file deletion and in recovering the erased tracks.

9. Forensics on the Networks

Computer forensics on the networks poses numerous challenges and difficulties due to the voluminous, transient and dispersed nature of the information on the network activities. This section describes how information on the network traffic could be collected and reconstructed for evidentiary purposes. In particular, the Netflow records, dialup server logs, network sniffer, TCP logs

and the various logs in the Unix and Windows operating system, address resolution cache at the datalink layer and intrusion detection system are valuable sources for finding digital evidence on the network activities. Similarly, there are also reliability and time synchronization problems related to these logs that the examiner must take into considerations. The final part of this section deals with network forensics on the application layer, such as emails, relay chat and the Internet.

10. Forensics on an Unknown Program

Identifying an unknown program requires analysis tools to study clues in the symbol tables and embedded strings in order to understand exploit code and backdoor code. Valuable information can be gathered from the system configuration, system and user programs, system and kernel memory, raw memory and the disk, or from the IP hostnames. This section also gives an example showing the determining of an unknown program that was installed through a compromised root account.

11. Forensics on Intrusion Activities

This section brings together the knowledge from the previous sections to perform forensic examinations on intrusion activities and reconstruction of the user activities. It looks at some of the unmistakable rootkit signatures and the tools and methods for collecting the digital evidence in areas such as program analysis, memory examination, remote network examination, process capture and system call trace. A forensic case example is also used in the latter part of the section to step through an investigation of a suspected intrusion, with follow up actions and a post mortem.

12. Forensics on Wireless Network

Forensic examinations on the wireless network centers mainly on the mobile phone network, covering areas such as the circuit switched wireless

network, the mobile device, the SIM card, the switching center, the various registries, the operational and maintenance center, encryption, billing database, wiretapping and location-based services. This section concludes with a brief description on the analysis of the 802.11 wireless local area network.

K. LABORATORY EXERCISES

Since computer security education and training is not an abstract academic discipline, it lends itself to the use of laboratory exercises. Formal classroom instruction needs to be augmented with case study analysis and projects necessary to impart such analytic and technical skills. [1] In addition, laboratory exercises help students understand and internalize key concepts. The use of tools and methods from both academic programs and industry can help instructors build useful laboratory programs to clarify the concepts and provide interesting challenges for the students.

The objective of the course is not to train students in the details of a particular product or to pass a standardized classroom test. Rather, the focus is on developing the students' analytical skills to tackle any computer security incidents that may arise. A set of laboratory exercises is thus designed to illustrate the computer forensic concepts being taught in class. Students will learn to use operating system tools and rootkits to extract useful digital evidence as well as lay their hands on professional computer forensic software.

L. SUMMARY OF THE LABORATORY EXERCISES

The laboratory manual is organized into seven sections covering the main topic areas in the course.

1. Foundstone Forensic Toolkit

The Foundstone Forensic Toolkit contains several Win32 command line tools to help examine files on an NTFS disk partition for unauthorized activity.

These open source tools scan the disk for hidden files and data streams, and list them with their MAC time without tampering the data attributes on the disk.

2. EnCase (Guidance Software)

EnCase is a powerful and non-invasive computer forensic tool featuring a graphical user interface that enables examiners to easily manage large volumes of computer evidence and view files, file slack and unallocated data. The integrated functionality of EnCase allows the examiner to perform all functions of the computer forensic investigation process, from the initial previewing of a target drive, the acquisition of the evidentiary images, the search and recovery of the data and the final reporting of findings, all within the same application.

3. AccessData Forensic Toolkit

The AccessData Forensic Toolkit (FTK) is a handy utility offering a complete suite for performing forensic examinations of computer systems. Its full text indexing offers quick advanced searching capabilities. Its deleted file recovery and file slack analysis are commendable. FTK is also interoperable with other AccessData utilities such as password recovery and encryption file identification programs. In addition, the FTK incorporates Stellent's Outside In Viewer Technology to access over 255 different file formats. The Known File Filter (KFF) feature can be used to automatically pull out benign files that are known not to contain any potential evidence and flags known problem files for the investigator to immediately examine. FTK can also support evidence files acquired by EnCase, Snapback, SafeBack and Linux DD.

4. Windows Event Log Analysis

Microsoft WinNT/2K can be configured to log events in binary files to record System events, Application events and Security events. These event logs store the descriptive messages in the registry and the separate executables or

dynamic link library files. The Event Viewer combines and displays the information in these files, providing a convenient way to view the data. Consequently, copying event log files from one system to another for examination may result in misinterpretation when viewing event logs on a remote system. The Event Viewers will read the event record data from the remote log files, but will search the registry of the local system for the corresponding event message files. Unless the forensic PC have similar configuration to the imaged system, it is necessary to extract all the registry keys and event message files from the image. By viewing the extracted logs using the Event Viewer, it is possible to create a short list of missing event message files and configure them in the forensic PC accordingly. Otherwise, the Event Viewer will not display explanatory material for any event for which there is no associated event message file.

5. DumpEvt (SomarSoft)

It is evident from the previous exercise, the clumsiness of performing manual Windows event log analysis on a remote forensic PC. Moreover displaying the logs using the Event Viewer is not very conducive for analysis since the Event Viewer is not integrated with other data processing tools. Besides, performing separate log analysis on individual machines in a networked environment does not readily link a related event across multiple machines. Rather, importing the contents of multiple machines' log files into a spreadsheet makes it easier to sort events chronologically and search the logs simultaneously. DumpEvt is a utility designed to dump multiple event logs in a format suitable for importing into a database to facilitate more event log analysis.

6. Unix Log Analysis

Unix serves as a wonderful training ground for computer security specialists. It teaches about access permissions for objects, builds on MS-DOS knowledge, and expands on MS-DOS piping and redirection capabilities. Using Unix scripting capabilities similar to DOS batch file, an investigator can create

combinations of commands into specialized programs to conduct security audits and to do granular file searching. The Unix system also has a comprehensive set of system configuration files that can prove to be an invaluable source of information.

7. Network Analysis

Analyzer is a fully configurable network analysis program for Win32 environment. It captures packets from network and displays them through a user-friendly graphical interface. Analyzer is capable of capturing packets from the network for real time monitoring and creating capture files. It allows the examiner to describe the protocol format, customize the display of the packets, evaluate statistics, plot graphs, set query on the analysis engine and set filter to record packets at the MAC, Network, Transport or Application Layer.

The intention of the laboratory exercise is not to spoon-feed students with step-by-step instructions on how to conduct a forensic examination. Rather, students will be expected to actively search for the relevant information, user instructions, software downloads, and put into practice the course concepts, in carrying out the exercises. This is to build up their resourcefulness and creativity towards tackling future forensic examinations. Pertinent technical guidance is included in each of the exercises in order to help them get started.

All the exercises will require students to have access to the Internet to download the software tools and if required, seek clarifications or technical support from the vendor on emails. However, this does not necessarily require the forensic machines to be connected to the external network. Rather, some of the exercises only require a standalone forensic machine with evidence already captured on a diskette, while others only require the forensic machine to be interconnected with the subject machines in a local area network. Implicit in the laboratory instructions is the preparation of the relevant evidence files by the laboratory technician for the students' forensic

investigations. Subject evidence issued to the student project groups shall preferably contain subtle differences between the groups to discourage duplications.

The laboratory exercise involving the EnCase forensic tool will require the forensic machine to be attached with a physical dongle on its parallel or USB port. This is a copyright protection feature. The user name and the corresponding password distributed with the licensed software are also necessary for downloading the latest software version of the forensic tool from the Guidance Software's website. All the other laboratory exercises are based on the inherent operating system utilities, freeware or demonstration software, which can be obtained from the relevant websites without cost. The demonstration software may include certain restrictions on its functionalities. Nevertheless, they are adequate for students to fulfill the laboratory requirements.

M. CONCLUSION

Becoming a computer forensic expert demands more training and experience than the brief introduction that can be afforded by this course. Computer forensics warrants technical expertise across a wide range of operating systems, hardware, and network devices and protocols. It is thus not the aim of this thesis to develop a course that will encompass all the necessary technical disciplines in order to produce graduates who will immediately become computer forensic experts. Rather it is hoped that the knowledge and laboratory exposure gained from the course will allow them to correctly respond to detected computer intrusions and unauthorized activities they may encountered on their C4I systems and facilitate those who aspire to become a full-fledged computer forensic expert, to start with by equipping them with the fundamentals in this specialized discipline of computer security.

APPENDIX A: LIST OF AGENCIES AND VENDORS PROVIDING COMPUTER FORENSIC COURSES AND TRAINING

1. AccessData Corporation
   www.accessdata.com

   AccessData Corporation has been doing business in the computer forensic and cryptography fields since 1987 and has established itself as a password recovery expert. Since then, AccessData has developed a trusted relationship with the US Government, state and local law enforcement, and corporate America. To help keep government agencies and corporate security departments up to date with current computer forensic technology, AccessData has developed training seminars to help both the novice and expert computer specialists.

   A 4-day Computer Forensic Training Class costs $1600 (not inclusive of software). The course covers basic computer forensic fundamentals and training on AccessData's Forensic Toolkit, Password Recovery Toolkit, and Distributed Network Attack Toolkit.

2. ASR Data Acquisition and Analysis
   www.asrdata.com

   ASR Data Acquisition and Analysis is a leading authority in the field of computer investigations by the United States Department of Justice. It provides software solutions, training and technical support to meet the needs of law enforcement agencies.

   ASR offers six computer forensic courses, namely the Data Acquisition Protocols Course, the Data Analysis Protocols Course and the Computer Crime Investigative Techniques Course for either DOS/Windows or Macintosh. These courses are geared toward the use of the Expert Witness, an automated computer forensic application created by ASR.

3. Berryhill Computer Forensic
   www.computerforensic.com

   Berryhill Computer Forensic provides computer forensic services to law enforcement agencies, attorneys, private investigators and businesses. It owns expertise and experience in handling evidence in criminal and civil cases, and also facilities to secure sensitive material. It caters mainly to law enforcement agencies in the Californian region. The Computer Forensic in Law Enforcement Course provides basic training in computer seizure procedures and computer evidence analysis for law enforcement officers.

4. CompuForensic
www.compuforensic.com

As a small business, CompuForensic offers computer forensic training in association with the Wright State University (WSU) in Ohio and Southern Methodist University (SMU) in Texas. CompuForensic specializes in the development of high quality computer forensic training. Previously restricted to full-time government employees or a select group of corporate security investigators, the computer forensic training is now available to the general public through the two universities.

A 4-day Basic Computer Forensic Initial Response Team Training costs $1995. It also includes the issue of commercially licensed software such as Norton Utilities, Quick View plus, Partition Magic, Norton Ghost and selected Maresware forensic utilities. The course is designed to equip computer investigators and analysts with the skills needed to safely locate and secure computer evidence at the search site.

A 4-day Advanced Computer Forensic Initial Response Team Training costs $1495 and employs the same software coupled with a major Linux distribution. A 1-day Program Manager's Course is designed for managers involved in supporting and supervising computer forensic operations.

5. Computer Sciences Corporation
www.csc.com

Computer Sciences Corporation (CSC) administers the Department of Defense Computer Investigations Training Program (DCITP) computer forensic program under contract to train the Department of Defense (DoD) criminal and counterintelligence investigators in computer forensic.

A 3-week Field Forensic Examinations curriculum is patterned after the Preparation, Preservation, Duplication, Investigation and Reporting (PPDIR) framework. It emphasizes on the evidence chain of custody and technical investigative software tools. Students are given three days to conduct an actual graded practical examination of a computer hard drive without technical assistance. Students also participate in a half-day mock trial where actual trial and defense attorneys question and cross-examine them on their findings from the graded examination.

6. Cranfield University, Royal Military College of Science
www.cranfield.ac.uk

The Center for Forensic Computing in Cranfield University, Royal Military College of Science (RMCS) is one of the very few institutions offering Forensic Computing postgraduate education leading to a Masters of Science

(3 years part-time program) or Postgraduate Diploma (2 years part-time program). It also offers short courses such as the Forensic Computing Foundation Course, Forensic Internet Course, and the Forensic Network Course. These 2-week short courses are also taught and discussed at the postgraduate level.

These courses provide an understanding of the principles and practical methods employed in the extraction of information for evidential purposes from computer systems. They examine how information may be stored in computer systems and how it may be deliberately hidden and subverted, thereby to gain an understanding of the methods and techniques used in the extraction of information for evidential purposes.

7. Department of Defense Computer Investigations Training Program
www.dcitp.gov

The Department of Defense Computer Investigations Training Program (DCITP) is dedicated to the development and delivery of computer investigative training for the following DoD elements: Defense Computer Forensic Lab (DCFL), Air Force Office Of Special Investigations (AFOSI), Naval Criminal Investigative Service (NCIS), Army Criminal Investigations Division (CID), Military Intelligence Group (IWB), Defense Criminal Investigative Service (DCIS). The DCITP offers a healthy variety of computer forensic short courses.

A 3-day Introduction to Computer Search and Seizure Course is designed to provide knowledge to properly seize and maintain the evidence value of computer media.

The System Administrator Incident Preparation and Response Course is a computer- based training distributed by Data Interchange Standards Association (DISA). It provides instructions in computer crime activities and specific practices to protect computer systems and support computer investigations.

The Basic Evidence Recovery Techniques Course is a scenario-based course for general computer-related crime. It includes extensive practice on imaging media on DOS and Windows 95/98. The course concludes with the creation of a case folder containing evidence for forensic analysis.

The Basic Forensic Examinations is a scenario-based course that focuses on media analysis. Principles of forensic analysis are presented with tools commonly used in the field, such as Encase. Students will learn preparation, image restoration, both FAT and NTFS file and directory structures, recovery of deleted files, and other analysis topics. The course concludes with the creation of a report detailing the forensic findings for the scenario.

The Incident Response in a Network Environment Course is a scenario-based course on network intrusions. Students will learn basic system administrator functions and extract information of evidentiary value from log files, user information and access rights. Students are given extensive practice on collecting images in a network environment.

The Managing Computer Investigations Course familiarizes students with the duties and activities common to the computer crime investigators.

The Field Investigations in a Solaris Environment Course prepares students to perform in-depth investigative functions in a Solaris operating system environment. This is a scenario-based course. Students will complete an investigation by performing forensic media analysis and log file analysis on a Solaris network.

The Field Investigations in a Windows NT/2K Environment Course prepares students to perform in-depth investigative functions in a NT/W2K operating system environment. Students will complete an investigation by performing forensic media analysis and log file analysis across a NT/W2K network.

8. DIBS USA Inc
www.dibsusa.com

DIBS USA Inc is a privately owned, independent corporation specializing in forensic computing, with activities in three main areas, namely the design, manufacture and supply of a range of computer forensic equipment; the provision of computer forensic analysis services and the training of investigators in computer forensic techniques and practice.

A 1-day intensive introductory course, Understanding Computer Forensic, costing $469, provides an overview in computer forensic theory and practice. This course is appropriate for professionals in related fields but not for those specializing primarily in computer forensic.

A 2-day course, Computer Forensic – The Essential Techniques, is designed to give a more solid foundation in the theory and practice of essential computer forensic techniques. The practical aspects of the course involves a number of simulated investigations on how to make image copies using the range of DIBS equipment for analysis and presentation to court. The course is suitable only for beginner with little previous experience or the more experienced computer operator wishing to learn basic forensic techniques. The fee for the course is $1130.

9. Federal Bureau of Investigation
www.fbi.gov

The Computer Training Unit (CTU) at the Federal Bureau of Investigation (FBI) Academy provides investigative computer instructions, training, and curriculum development to FBI and other foreign law enforcement personnel. Primarily, CTU trains its students on how to use the computer as an investigative tool, computer fraud, computer crimes, intrusions, search and seizure of computer as well as how to use the computer as a source of information.

10. Federal Law Enforcement Training Center
www.fletc.gov

The Federal Law Enforcement Training Center (FLETC) serves as an interagency law enforcement training organization for numerous Federal agencies throughout US. The center also provides services to state, local and international law enforcement agencies.

The Seized Computer Evidence Recovery Specialist Training Program introduces the concept of automated data processing and the techniques and procedures for investigative computer search, seizure and analysis issues of a multitude of operating systems. The curriculum also addresses the legal issues related to computer evidence.

11. Foundstone
www.foundstone.com

With a combination of outstanding personnel and industry-leading methodologies, Foundstone delivers computer-security services in consulting and education. It provides professional services in penetration testing, e-commerce application testing, incident response and computer forensics, product testing, wireless security testing as well as expertise in Microsoft environments utilizing ISA Server technology.

A 4-day Incident Response & Computer Forensic Course deals with forensic techniques to recognize, respond to, and recover from insider and outsider attacks. Students learn the science of incident response through presentations and hands-on lab exercises. This includes an in-depth study of the computer forensics process from creating evidentiary disk images to recognizing the often-faint trail of unauthorized activity. Students will also learn step-by-step incident-response procedures for Unix and Windows NT/2K. Lab Exercises include forensic analysis of victimized systems, review of network traffic and intrusion-log, review of backdoor tools that circumvent intrusion-detection systems, determining the function of unidentified processes, detection of

loadable kernel modules, rootkits and trojans. The course costs $3500.

12. Fred Cohen & Associates
www.all.net

Fred Cohen & Associates is one of the world's leading researcher and corporate consultant in the area of information protection. It specializes in top-level assessment of corporate protection programs, strategic scenario development for national policy decisions, risk management support for large multinational corporations, strategic program planning, Internet firewall suitability assessments, electronic commerce architecture analysis and effectiveness testing for critical infrastructure elements.

The Digital Forensic Course is a self-paced CD-ROM instruction providing a comprehensive overview of digital forensic with a slight focus on the Unix operating environment and examples from many other sorts of systems. It includes viewgraphs covering a wide range of topics in digital forensic, audio recordings and examples from real cases. A copy of the CD-ROM costs $249.

13. Guidance Software
www.guidancesoftware.com

Guidance Software is one of the leaders in computer forensic software, acquisition hardware and training. Guidance Software is well known for developing EnCase, a comprehensive software that handles every stage of computer forensic investigations, from the preview and acquisition of an evidence drive to the generation of a final report.

Guidance Software offers three training courses on the EnCase Computer Forensic Methodology at the introductory, intermediate and advanced level. The introductory course introduces students to the field of computer forensic. The intermediate course addresses data recovery techniques. The advanced course involves advanced data recovery techniques and an in-depth study of file systems. The course fees for each of the 4-day course are $2000, $2500 and $3000 respectively.

14. High Tech Crime Consortium
www.hightechcrimecops.org

The High Tech Crime Consortium (HTCC) provide practical information and hands-on training on evidence seizure, handling and storage, legal requirements and search warrant preparation, computer criminal behavior analysis and guidelines for planning, personnel considerations, field seizure team development

The HTCC proposal for a Certificate in Computer Forensic consists of 45

quarter hours curriculum for basic computer forensic, high technology incident response, high technology vulnerability assessments, risk management and high technology infrastructure protection management. Two other specialty courses, Computing Forensic I and Computing Forensic II are taught using computer-based instructions.

15. High Tech Investigators Association
www.htcia.org

The High Technology Crime Investigation Association (HTCIA) is an organization designed to encourage, promote, aid and effect the voluntary interchange of data, information, experience, ideas and knowledge about methods, processes, and techniques relating to investigations and security in advanced technologies among its membership. It organizes regular computer forensic training conferences for law enforcement personnel under its Regional Training Program. These training conferences are restricted only to law enforcement personnel.

16. High Tech Crime Network
www.htcn.org

The High Tech Crime Network (HTCN) issues certifications on a variety of high tech crime related topics through courses provided by its list of approved agencies, organizations or companies. HTCN does not directly provide such training. Rather, it offers both basic and advanced certifications for Certified Computer Crime Investigator, Certified Computer Forensic Technician, Certified Computer Crime Prosecutor, Certified Computer Crime Attorney and the Certified Network Security Professional. These certifications are issued as a result of acquiring the required experience, course hours and successfully completing a written test. They serve to provide a higher degree of professionalism and continued training and support within the high tech crime industry. The cost for each of the certifications is $250.

17. Institute of Police Technology and Management, University of North Florida
www.iptm.org

The Institute of Police Technology and Management (IPTM), University of North Florida is established to provide specialty training to law enforcement agencies in community policing.

A 5-day Computer Crime Investigations Course is designed to train law enforcement investigators in the latest techniques of modern computer crime investigation. The course includes practice on preparing search warrant documents for the seizure of a suspect's computer, how to image and examine the system for evidence relating to a criminal offense, and how to present this evidence for prosecution. It also includes the use of the Internet to conduct

follow-up investigative work pursuant to an ongoing investigation. The cost fee is $795.

18. International Association of Computer Investigative Specialists
www.cops.org

The International Association of Computer Investigative Specialists (IACIS) is a volunteer non-profit corporation composed of law enforcement professionals dedicated to education in the field of forensic science. The international computer investigative organization provides both a network for trained investigators and an annual basic training conference for law enforcement professionals.

The Law Enforcement Computer Forensic Training is a 2-week course costing $1395. It consists of both classroom and hands-on training. The course outlines generic computer crime investigations, such as interpreting and tracing email, identification of electronic evidence and the proper collection method to preserve the integrity of such evidence. The course also includes sector level examination and analysis of hard disks and removable media, data recovery, identification and handling of data destructive software schemes, encryption theory and decryption techniques. After completion of the 2-week course, a basic examiner is required to complete a set of forensic investigation problems via home study before receiving certification. The students are given one year to complete the hands-on technical examinations on the issued computer media without the use of any automated forensic processing software.

19. International Association of Directors of Law Enforcement Standards and Training
www.iadlest.org

The International Association of Directors of Law Enforcement Standards and Training (IADLEST) is an international organization whose mission is to research, develop and share information, ideas and innovations in establishing effective and defensible standards for employment and training of law enforcement officers. Its primary focus is criminal justice standards and training. It does not directly conduct any formal computer forensic training, but offers a list of computer forensic courses conducted by the Law Enforcement Training Center, the Police Training Institute, and the Institute of Police Technology and Management.

20. Internet Crimes, Inc
www.internetcrimes.com

Internet Crimes, Inc is a subsidiary of PowerPhone, Inc. It offers on-site, hands on training for law enforcement agents, government officials, attorneys,

and computer security professionals in the area of Internet crime investigations. Its staff includes computer crime investigators and attorneys who have worked on computer crimes cases. Internet Crimes, Inc. is one of the official training provider for the High Technology Crime Network (HTCN).

A 5-day Computer Crime Investigators Certification Program costs $649. The topics covered include examples of computer crimes, introduction to computer forensic, computer evidence collection and crime specific investigations.

A 3-day Computer Fraud and Financial Crime Investigation Program costs $599. Topics covered include introduction on theft of identity, intellectual property, fraud, piracy, scams, counterfeiting and the relevant investigative tools and techniques.

21. Key Computer Service, Inc
www.keycomputer.net

Key Computer Service, Inc. is a small corporation that specializes in computer forensic. It has a full range of technical and investigative expertise providing computer forensic examination, data recovery, password recovery and other electronic data services. In addition, it also provides self-paced on-line training in computer forensic and data recovery.

The Computer Forensic Course is broken up into five modules and the fee for the on-line instructions is $2250. The course covers processes and methodologies to conduct forensic examinations and the recovery of evidence and data from magnetic media with the use of specially prepared practical exercises. The practical exercises will require students to create and verify forensically sterile examination media, to create forensic boot diskettes, to make forensic copies of media, to find and recover deleted, formatted, hidden and lost data, to access mail, cache and other internet related files, to unlock passwords, data format conversion, to provide opinions regarding examinations and a complete hands-on examination of a specially prepared hard disk drive with real life forensic issues. Software provided as part of the course includes the Wiper, FreeSecs and DiskDupe disk utilities, ListDrv and ChkSum.

The Data Recovery Course is broken into three modules and the fee for the on-line instructions is $1650. The course covers physical crash recovery techniques, as well as data recovery from raw media that has no directory or sub-directory listings. The on-line instruction is also accompanied with related practical exercises.

22. Knowledge Solutions Campus
www.forensic-science.com

Knowledge Solutions specializes in delivering on-line instructions on forensic science. It has onboard, qualified and experienced instructors who have done leading edge casework in their fields. One of the instructors is Eoghan Casey, an author and editor of several books on computer forensic. Lesson plans and assignments are posted weekly as web pages with web-based discussion forum to allow interaction among fellow students and the instructor, post questions and exchange ideas. Students are expected to spend about 5 hours per week for the on-line instructions.

Knowledge Solutions offers a range of courses on forensic sciences, and four modular courses specifically on computer forensic. The Introduction to Internet Crime Course, and the Introduction to Digital Evidence and Computer Crime Course are both 3-week long, each costing $75. The Investigating Internet Crime Course and Advanced Digital Evidence Course are 10-week long and cost $225 each. These courses are based on material in Eoghan Casey's book on Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet.

23. Kroll
www.krollworldwide.com

Kroll is a leading risk-consulting company offering professional services in analysis of intelligence, assessment of threats and implementation of measures to offset risks relating to a wide range of current and potential difficulties. They include internal controls, employee or vendor malfeasance, threats to corporate security, intellectual property theft, and financial improprieties.

The Kroll Information Security Group provides a variety of courses designed for forensic and network investigative certifications. The Introduction to Technology Crime/First Responder Course is a 5-day introductory program to the field of technology crime. At the conclusion of the course, students will be able to recognize the occurrence of technology crimes, as well as preserve and collect necessary items of evidence. The cost for the course is $1595. The Computer Forensic Course is a 5-day program at $1695. It covers the fundamentals of forensic investigations. The Internet Investigation Course introduces students to the configuration and operations of the Internet and techniques for conducting investigations on the Internet. The 5-day program costs $1595. The LAN Investigation Course introduces students to the principles of computer networks, common network configurations and some of the considerations that investigators need to consider when they encounter computer networks. The 5-day program costs $1695. The Electronic Discovery and Forensic, Continuing Legal Education Course is an 8-hour

custom seminar to present attorneys with a familiarization to computer forensic and electronic recovery.

24. LC Technology International, Inc
www.lc-tech.com

LC Technology International, Inc is a developer of PC-based utility software. As the end-user market increases and users become more sophisticated, LC Technology is experiencing large increases in sales outside of its core business. Its core product line is designed to fill the security needs of data protection, recovery and security of digital data. LC Technology offers a series of 3-day course costing $1250 each.

Both the Basic and Advanced Computer Forensics Course are designed to train corporate and law enforcement investigators in the basic elements of computer forensic investigation. Through hands-on practice, students will learn how to properly seize and examine an IBM-based PC and related media for evidence relating to a criminal or civil offense.

The Homeland Defense Digital Investigations Program is designed to train corporate and law enforcement investigators in computer and digital investigations relating to domestic terrorism suspects. Students will conduct examinations of digital media captured from actual domestic terrorism cases and will work as a team to develop credible intelligence. Emphasis will be placed on the recovery and examination of terrorist e-mails and the use of encryption by terrorist cells.

The Investigating Internet Crimes Against People Program includes a statutory overview of Internet and computer crimes, setting up an on-line Investigation, a hands-on laboratory simulating an internet investigation, acquiring and preserving digital evidence. During the exercise, students will use the data recovery and forensic tools, and learn the techniques to conduct a thorough computer forensic exam for a courtroom presentation.

25. Mares and Company, LLC
www.dmares.com

Mares and Company, LLC is a small company that provides computer forensic examinations and periodically hosts computer forensic and MARESWARE training seminars to state and local law enforcement.

A 5-day Basic Computer Forensic Seminar costs $1000. The topics covered include search warrant wording, creating forensic boot disks undeleting files, preserving disk evidence, forensic processing, imaging and copying procedures.

A 2-week Advanced Computer Forensic Seminar cost $2000. It covers more complex topics and include more hands-on and practical exercises such as in depth command line usage and designing complicated script batch files, disk editing, preserving disk evidence, forensic processing, hashing techniques, disk cataloging, imaging and copying procedures, process validation and automating the seizure process.

A 5-day Maresware Forensic Software Computer Training cost $800. The topics covered include how to use Maresware forensic software for performing forensic analysis of computers with a significant amount of hands-on practice using the Maresware forensic software. Students will practice with and become familiar with the capabilities of the software, thus developing a better understanding of what the software is capable of and how to use it more efficiently when doing forensic and data analysis.

26. National White Collar Crime Center
www.cybercrime.org

The National White Collar Crime Center (NW3C) is a non-profit organization funded by the Department of Justice, Bureau of Justice Assistance. It provides support to local and state enforcement agencies involved in the prevention, investigation, and prosecution of economic and high-tech crime. It conducts a Basic as well as an Advanced Data Recovery and Analysis Course. These 5-day courses are sponsored by the National Cybercrime Training Partnership (NCTP). There is no fee for the courses and they are open only to law enforcement personnel.

The Basic Data Recovery and Analysis Course includes hands-on instructions and discussion about evidence identification and extraction, hardware and software needed to do a seizure, how to recover erased files, how to overcome encryption and high-tech legal issues. The Advanced Data Recovery & Analysis Course takes the students into more varied and complex technical areas such as large hard drives, new partition types, long file name and date stamp issues, FAT, NTFS, advanced imaging, alternate media, transient data, internet issues and testimony considerations.

27. New Technologies, Inc
www.forensic-intl.com

New Technologies, Inc (NTI) provides consulting services to large law firms and corporations concerning e-commerce evidence and general computer evidence issues. NTI also provides software tools and advisory services to military and intelligence agencies in computer security risk identification and on the elimination of such risks. Its primary expertise lies in the development of state-of-the-art computer forensic and risk assessment tool, computer forensic training and computer evidence consulting.

A 1-day Data Imaging Course deals specifically with issues related to creating evidence grade bit stream copies of computer hard disk that may contain electronic evidence. The training course will include detailed instructions and hands-on experience in using NTI's forensic tools developed for the bit stream backup imaging process. These tools, provided with the course, include SafeBack, Disk Scrub and M-Sweep.

A 1-day Forensic Training Course is intended as an overview of computer evidence processing techniques and the use of NTI's automated computer forensic software. The software provided with the course includes DiskSig, CrcMD5 and NTIDoc documentation tool.

A 3-day Computer Forensic Course deals specifically with DOS and Windows 95/98/ME. It covers evidence preservation, evidence processing methodologies and computer security risk assessments in detail. Recently, the course content has been expanded to support US Government's needs on computer incident responses and computer forensic binary data searches for foreign language computer data. This hands-on training course exploits the inherent security weaknesses of the operating systems to find computer evidence and security leakage of sensitive data. The students will receive a suite of NTI forensic software. The course costs $2295.

A 2-day Network Forensic Course is intended to supplement the 3-day Computer Forensic Course and deals specifically with the Windows NT/2000. The course includes instructions and hands-on experience in using the NTI forensic tools on the processing and analysis of NTFS related evidence. They include PTable, DiskSearchNT, GetSlackNT, GetFreeNT, NTICopy and FileListNT. Students will receive a copy of these specialized forensic tools.

28. Ohio Peace Officer Training Academy
www.ag.state.oh.us/opota/opota.htm

The Ohio Peace Officer Training Academy (OPOTA) is administered by the Attorney General through the Ohio Peace Officer Training Commission. The commission establishes uniform courses of training for law enforcement officers and private security throughout Ohio. It offers training subjects ranging from criminal investigation to the use of firearms. All the computer forensic courses offered by OPOTA are restricted to active law enforcement only.

A 4-day Basic Computer Data Recovery Course is designed for law enforcement personnel responsible for forensic data recovery from seized computers. The course emphasizes the safe preservation and recovery of computer evidence. The course fee is $375.

A 5-day Intermediate Computer Forensic Course is designed to prepare law enforcement personnel for more advanced investigations on systems such as Windows NT/2K, Unix and Macintosh, data recovery from networks and other advanced problems generally faced by computer forensic specialist. The course fee is $275.

A 4-day Internet Investigation Course is designed for law enforcement personnel responsible for investigating crimes involving the Internet. Topics include case preparation, email and IP tracing, viruses and introduction to intrusions. The course fee is $225.

29. University of New Haven
www.newhaven.ed

The University of New Haven offers on-line courses for undergraduate and graduate credit toward degrees in criminal justice in the areas of forensic computer investigation and information protection and security. Among its faculty is Fred Cohen, who is best known as the inventor of computer viruses and virus defense techniques.

The Certificate in Forensic Science/Forensic Computer Investigation requires 12 academic credits from a list of related on-line courses such as Computer Crime, Legal Issues and Investigative Procedures Computers, Technology and Criminal Justice Information Management Systems, Advanced Crime Scene Investigation. Each of the 3-credit on-line course costs $1335.

30. Veridian
www.veridian.com

Veridian is a designer and operator of secure, intelligent network environments. Leveraging 25 years of experience gained from protecting important components of the country's communications infrastructures, Veridian offers a full suite of leading-edge network and information security services and products. As a knowledge applications provider, it develops integrated systems and applications, establishes secure network environments to make intelligent decisions.

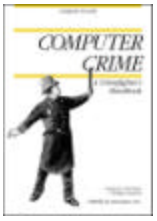
A 10-day Macintosh Forensics Analysis Course provides a short overview of the Apple hardware and software, the Macintosh 9.0.4 operating system and highlights system functions and features that are important for a forensic examination. Students will learn how to map a Macintosh hard drive and learn places to discover hidden data. Students will also learn to use selected software tools during the hands-on exercises. The fee for the course is $5190.

APPENDIX B: LIST OF READINGS ON COMPUTER FORENSICS

1. Avoiding Cyber Fraud in Small Businesses: What Auditors and Owners Need to Know
by Jack Bologna, Paul Shaw and G. Jack Bologna
John Wiley & Sons, May 2000

This book provides critical guidance on what auditors and businesses can do to prevent and detect the most rapidly growing kind of fraud—cyber fraud. Here, auditors, business owners and managers—the ones being held accountable when this kind of criminal activity is detected—will learn how to beware of the dangers of internal theft by computer, illegal access to information systems, credit card frauds, Internet scams and insure that adequate controls are in place for its prevention and detection.

2. Computer Crime: A Crimefighter's Handbook
by David J. Icove, David Seger Karl Icove, Karl A. Seger and Vonstorch
O'Reilly & Associates, Inc.



Terrorist attacks on computer centers, electronic fraud on international funds transfer networks, viruses and worms in software, corporate espionage on business networks, and crackers breaking into systems on the Internet. Computer criminals are becoming ever more technically sophisticated, and it's an increasing challenge to keep up with their methods. The book is for readers who need to know what today's computer crimes look like, how to prevent them, how to detect, investigate and prosecute them if they do occur. It contains basic computer security information as well as guidelines for investigators, law enforcement, computer system managers and administrators.

The book contains a discussion on computer crimes, the computer criminal and computer crime laws. It describes the various categories of computer crimes and profiles the computer criminal using techniques developed for the FBI and other law enforcement agencies. It outlines the risks to computer systems and personnel, operational, physical, and communications measures that can be taken to prevent computer crimes. It then discusses how to plan for, investigate, and prosecute computer crimes, ranging from the supplies needed for criminal investigation, to the detection and audit tools used in investigation, to the presentation of evidence to a jury. It also contains a compendium of the computer-related US federal statutes and all of the statutes of the individual states, as well as representative international laws.

Lastly, the book contains a resource summary, detailed papers on computer crime and a sample search warrant for a computer crime.

3. Cyber Crime Investigator's Field Guide
by Bruce Middleton
CRC Press, December 2001

This book provides the details of investigating computer crime and the chain of evidence from what to do upon arrival at the scene until the investigation is complete. It covers information such questions to ask the client, steps to follow when arriving at the client's site, procedures for collecting evidence, details on how to use various evidence collection and analysis tools, and how to recover lost passwords or documents that are password protected. It also includes case studies on computer forensic tools in action, commonly used Unix/Linux commands, port number reference for various services and applications, computer forensic software tools commands synopsis, attack signatures and Cisco PIX firewall commands. The author provides an investigative framework, knowledge of how cyberspace really works and the tools to investigate cyber crime.

4. Computer Forensics
by Warren G. Kruse II and Jay G. Heiser
Addison-Wesley Publishing Company, September 2001

The book offers a disciplined approach to implementing a comprehensive incident-response plan, with a focus on how to detect intruders, discover what damage they did and find out who they are. The bulk of the book details the technical skills and emphasis on providing a well-documented basis for a criminal investigation. The key to success is becoming a "white hat" hacker in order to combat the criminal "black hat" hackers. In this vein, the authors use a number of technical examples and encourage readers to develop expertise in Unix/Linux and Windows NT fundamentals. They also provide an overview of a number of third-party tools, many of which can be used for both tracking hackers and to probe the users' own systems. Frequent examples are used to demonstrate how to extract evidence from a violated computer system.

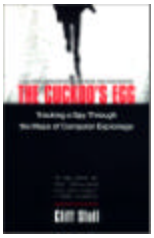
5. Computer Forensics: Computer Crime Scene Investigation
by John R. Vacca
Charles River Media, December 2001

This book provides a comprehensive overview of computer forensics from its definition to crime scene investigation, seizure of data, determining the fingerprints of the crime and tracking down the criminal. The book focuses on solving the crime rather than information security. Case studies and vignettes of actual computer crimes are used. The enclosed CD includes demonstrations on the latest computer forensics and auditing software.

6. Computer Forensics and Privacy
(Artech House Computer Security Series)
by Michael Caloyannides
Artech House, September 2001

The book delivers a comprehensive treatment on the threats to data confidentiality posed both by the emerging field of computer forensics and by connecting a computer to the Internet. It provides valuable critical information on identifying the specific areas where sensitive and potentially incriminating data is hiding in personal computers and explains how to go about removing this data; on install operating systems and application software that will help to minimize the possibility of security compromises; on ensuring computers that are connected to the Internet are protected from malicious mobile code and the new fashion of "adware/spyware", and on detecting whether advanced investigative tools, such as keystroke storing and relaying hardware and software, are in use in a computer. Other key topics include the pitfalls of encryption and how to use it effectively, the practical aspects of online anonymity and the current legal issues that pertain to the use of computers. Over 70 illustrations emphasize major points throughout the book.

7. Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage
by Clifford Stoll
Pocket Books, October 2000



A sentimental favorite, this book has inspired a whole category of books exploring the quest to capture computer criminals. Several years after its initial publication and after much imitation, the book remains a good read with an engaging story line and a critical outlook, as the author becomes a one-man security force trying to track down faceless criminals who have

invaded the university computer lab he stewards. What first appears as a 75-cent accounting error in a computer log is eventually revealed to be a ring of industrial espionage, primarily thanks to the author's persistence and intellectual tenacity.

8. Cyber Crime: How to Protect Yourself from Computer Criminals
by Laura E. Quarantiello
Tiare Publications, December 1996

The author offers a detailed look at what is happening in the world of computer crime, complete with insights into the minds of the perpetrators—from the mischievous to the malicious. Her stories include both the disturbing and the heartening, and the advice she has collected—from cyber-cops and cyber-criminals alike, is well worth heeding. Readers will learn about the three-step scale of vulnerability, cyber-cops, how they walk the digital beat and view intimate portraits of hackers and the tools they use.

9. Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes
by Albert J. Marcella Jr (editor) and Robert S. Greenfield
Auerbach Publications, December 2001

The book provides a comprehensive, highly usable and clearly organized resource to the issues, tools and control techniques needed to successfully investigate illegal activities perpetuated through the use of information technology. This book introduces the broad field of cyber forensics and presents the various tools and techniques designed to maintain control in an organization. It dwells on how to identify inappropriate uses of corporate IT, examine computing environments to identify and gather electronic evidence of wrongdoing, secure corporate systems from further misuse, identify individuals responsible for engaging in inappropriate acts, and protect and secure electronic evidence from intentional or accidental modification or destruction. Knowing how to identify, gather, document, and preserve evidence of electronic tampering and misuse makes reading this book and using the forensic audit procedures it discusses essential to protecting corporate assets.

10. Defending Your Digital Assets Against Hackers, Crackers, Spies, and Thieves
by Randall K. Nichols, Daniel J. Ryan, Julie J. C. H. Ryan and Arthur W. Jr. Coviello
McGraw-Hill Professional Publishing, December 1999

This is a guide to computer security. In place of specific how-to information,

readers learn about the motives of on-line attackers and the strategies they use to gain unauthorized access to systems and data, plus overarching concepts like public-key cryptography. It also deals about defensive and forensic strategies for preventing attacks and limiting their potency when they occur. The topics covered include computer and network security, risk management, security policy, cryptography, access control, authentication, biometrics, actions to be taken during an attack and case studies of hacking and information warfare.

11. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet
by Eoghan Casey
Academic Press, March 2000

Many readers commented that this is one of the best computer forensic book describing the elements of digital crime. The book is clear and easy to understand. The author applies the methodology of forensic science to computer crime investigations. The book begins with an explanation of how the computer functions, how they can be used in crime and how the evidence created from these activities can be used for later analysis. The accompanying CD-ROM contains simulated cases to integrate the topics covered in the text. This book is used as a training text at the Atlanta ISSA.

12. Disk Detective - Secrets You Must Know to Recover Information from a Computer
by Norbert Zaenglein
Paladin Press, September 1998

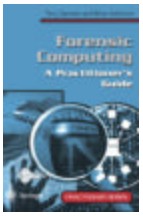
This book is designed to bring the secrets of information recover to the average person. In it, the author shows private investigators, parents, teachers, business owners and law enforcement professionals what types of information can be recovered from IBM-compatible personal computers and how. He includes step-by-step instructions for recovering information from reformatted disks or overwritten files, retrieving deleted files, discovering passwords and retracing visited Internet files.

13. Fighting Computer Crime: A New Framework for Protecting Information
by Donn B. Parker
John Wiley & Sons, August 1998

A revolutionary new approach to computer security. In this book, the author first shows why current approaches to preventing computer crime are not

working, and then presents a new framework for understanding criminal threats, describing proven countermeasures and discussing actual crime cases. Boldly critiquing many prominent business and government figures for their failings, this book pulls no punches in its drive to improve information security.

14. Forensic Computing: A Practitioner's Guide (Practitioner Series)
by Tony Sammes, Brian Jenkinson and A. J. Sammes
Springer Verlag, October 2000



In this book, the authors show how information held in computer systems can be recovered and how it may be deliberately hidden or subverted for criminal purposes. The content is illustrated by plenty of case studies and worked examples and will help practitioners and readers gain a clear understanding of how to recover information from computer systems in such a way as to ensure that its integrity cannot be challenged and that it will be accepted as admissible evidence in court; the principles involved in password protection and data encryption; the evaluation procedures used in circumventing these safeguards; the particular legal issues associated with computer-generated evidence and how to ensure admissibility of such evidence. This is a text aimed at helping practitioners get to a level of technical understanding that would allow them to be able to use forensic computing analysis to search for, find and present any form of digital document as evidence in court.

15. Handbook of Computer Crime Investigation: Forensic Tools & Technology
by Eoghan Casey (editor)
Academic Press, October 2001

Following on the success of his introductory text, Digital Evidence and Computer Crime, the author brings together the specialized knowledge of a few top experts to create the first detailed guide for professionals who are already familiar with digital evidence. This book helps readers master the forensic analysis of computer systems with a three-part approach covering tools, technology and case studies. The Tools section provides the details on leading hardware and software programs—such as EnCase, Dragon and ForensiX—with each chapter written by that product's creator. The section ends with an objective comparison of the strengths and limitations of each tool. The main Technology section provides the technical "how to" information for collecting and analyzing digital evidence in common situations, starting with computers, moving on to networks and culminating with embedded systems. The Case Examples section gives readers a sense of the technical, legal and practical challenges that arise in real computer

investigations.

16. High Technology Crime Investigator's Handbook
by Gerald L. Kovacich and William C. Boni
Butterworth-Heinemann, September 1999

This book informs readers about the potential of high tech crimes and the resources that are available to combat them. The book covers the management of a high tech investigation unit. The authors provide an overview of the entire high-technology crime investigation process. The book not only deals with a myriad of important issues but also offers viable solutions and prevention programs.

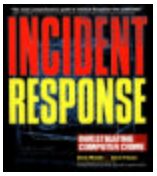
17. Incident Response
by Richard Forno, Kenneth R. Van Wyk and Rick Forno
O'Reilly & Associates, July 2001

This book introduces the modes of attack and the methods of response. The authors explain the organization and function of the professional, governmental and ad hoc groups that exist to respond to attacks and disseminate information about them. The topics covered include tools and strategies hackers use to break into systems illegally, and mechanisms and procedures for dealing with such attacks. Emphasis falls on the business considerations associated with incident preparedness and response.

18. Incident Response: A Strategic Guide to Handling System and Network Security Breaches
by Russell Shumway and E. Eugene Schultz
New Riders Publishing, January 2002

This book teaches readers what they need to know to not only set up an incident response effort, but also how to improve existing incident response efforts. The book provides a comprehensive approach to incident response, covering everything necessary to deal with all phases of incident response effectively, spanning from pre-incident conditions and considerations to the end of an incident. It also covers the technical considerations, what needs to be inspected in case they are corrupted, the types of logging data available in major operating systems and how to interpret it to obtain information about incidents, and how network attacks can be detected on the basis of information contained in packets. The major focus of this book is on managerial and procedural matters. It advances the notion that without effective management, incident response cannot succeed.

19. Incident Response: Investigating Computer Crime
by Chris Prosise and Kevin Mandia
McGraw-Hill Professional Publishing, June 2001

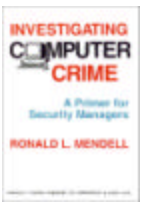


Written by FBI insiders, this book reveals the computer forensics process and offers authoritative solutions designed to counteract and conquer hacker attacks. It teaches the readers how to determine when an attack has occurred or is underway and what to do about it. The authors favor a tools- and procedures-centric approach to the subject, thereby distinguishing this book from others that catalog particular attacks and methods for dealing with each one. Their approach is more generic and therefore better suited to dealing with newly emerging attack techniques. Anti-attack procedures are presented with the goal of identifying, apprehending and prosecuting attackers. The advice on carefully preserving volatile information, such as the list of processes active at the time of an attack, is easy to follow. The book is quick to endorse tools and the functionalities of which are described so as to inspire creative applications. Information on bad-guy behavior is top quality as well, giving readers knowledge of how to interpret logs and other observed phenomena. The authors do not offer a foolproof guide to catching crackers in the act, but they do offer a great "best practices" guide to active surveillance.

20. Investigating Computer Crime
(CRC Series in Practical Aspects of Criminal and Forensic Investigations)
by Franklin Clark, Ken Diliberto (contributor) and Vernon J. Geberth (editor)
CRC Press, July 1996

This book presents practical methods for gathering electronic evidence and dealing with crimes involving computers. It follows a step-by-step approach to the investigation, seizure and evaluation of computer evidence. The material in the book has been used at the Federal Law Enforcement Training Center (FLETC), the Canadian Police College for teaching computer classes in white-collar crime and sex crime investigations and by US Army Intelligence in cooperation with NATO in Europe. It has also been used to teach a 1-week course in computer crime investigation to agents from the IRS, Secret Service, and state and local agencies.

21. Investigating Computer Crime: A Primer for Security Managers
by Ronald L. Mendell
Charles C Thomas Pub Ltd, September 1998

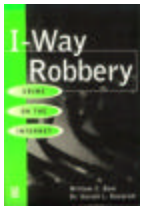


This book provides a fundamental investigative foundation for law enforcement and security managers by moving through the basic phases of a computer crime investigation. Topics include: solvability factors; retail computer security; intelligence gathering; the investigative process; establishing the corpus delicti; preserving evidence; determining the evidence, weak points and responsible parties; and deciding on a course of action. Ideas for discussion follow each chapter, providing material for in-depth exploration of the topics presented. The appendix contains a wealth of knowledge on information warfare, extremists and other threats from cyberspace.

22. Investigating Computer-Related Crime: A Handbook For Corporate Investigators
by Peter Stephenson
CRC Press, September 1999

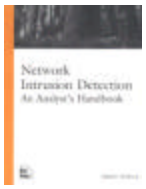
Written by an experienced information security specialist, this book offers a step-by-step approach to understanding and investigating security problems, technical and legal information, and computer forensic techniques. It discusses the nature of cyber crime, its impact in the 21st century, its investigation and difficulties encountered by both public law enforcement officials and private investigators. It gives advice on collecting and preserving evidence, interrogating suspects, handling crime in progress and in involving authorities.

23. I-Way Robbery: Crime on the Internet
by William C. Boni, Gerald L. Kovacich and John P. Kenney
Butterworth-Heinemann, May 1999



This book offers a basic understanding of Internet crime and covers related Internet business, government, political and privacy issues. It describes techniques used to commit crimes, what can be done about them, what challenges the future may hold, discusses real world problems and solutions for both technical and non-technical professionals, and analyzes actual Internet crime cases. This book is for security professionals who need to get up to speed on the whole issue of crime on the Internet. This book explains the history of the Internet, the future of it and to which it can expose an organization.

24. Network Intrusion Detection: An Analysts' Handbook
by Stephen Northcutt
New Riders Publishing, August 1999



This book explains what readers need to know to prevent unauthorized accesses of networked computers and minimize the damage intruders can do. It emphasizes proven techniques for recognizing attacks while they are underway. The author explains ways to spot suspicious behavior and deal with it, both automatically and manually. He explains SYN flooding and TCP hijacking with clarity and detail. Readers will get a good picture of the famous Kelvin Mitnick's attack and how Tsutomu Shimomura's server reacted. He also explains how a system administrator would detect and defeat a Mitnick attack. Another case study shows how a bad guy with root privileges attacked a DNS server.

25. Secret Software: Making the Most of Computer Resources for Data Protection, Information Recovery, Forensic Examination, Crime Investigation and More
by Norbert Zaenglein
Paladin Press, July 2000

Norbert Zaenglein, author of the best-selling book Disk Detective, takes the software secrets that have been the exclusive domain of hackers and other computer-savvy surfers mainstream. In straightforward, non-technical terms, the book covers an array of computer resources: electronic document shredders, a new electronic truth serum that rivals the polygraph, detection and identification of electronic intruders, professional forensics software and image enhancement software to assist in law enforcement investigations, file viewers that provide instant access to files that cannot be opened, and computer security programs. However, one reader ever described this book as basically an advertisement for software.

26. Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace
by Richard Power
Que, August 2000

Between interviews with hackers and security experts, the author suggests that the world's networks are swarming with money-sucking leeches, most of which are never even noticed, and certainly not caught. He delves into the twists and turns of the criminal investigations and the motivation of cyber-crooks. The author also gives credit to law enforcement agencies and security consultants who have made genuine progress in preventing crime and apprehending criminals.

27. Transnational Criminal Organizations, Cybercrime, and Money Laundering: A Handbook for Law Enforcement Officers, Auditors, and Financial Investigator
by James R. Richards
CRC Press, December 1998

Written by a law-enforcement professional, this book examines the workings of organized criminals and criminal groups that transcend national boundaries. Discussions include methods used by criminal groups to internationally launder money; law enforcement efforts to counteract such schemes; and new methods and tactics to counteract transnational money laundering.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C: LIST OF TOOLS FOR COMPUTER FORENSIC INVESTIGATION

1. Computer Forensics Software
from The Coroner's Toolkit
www.cerias.purdue.edu/homes/carrier/forensics

The Coroner's Toolkit (TCT) is a collection of tools oriented towards gathering or analyzing forensic data on a Unix system.

TCTUTILs is a collection of utilities in the TCT. It lists directory inode contents to view file, device, and directory names. This allows deleted file names to be viewed and with some platforms, an entire deleted file can be easily recovered. It can obtain Modified, Accessed, and Created time data on deleted files. It can also display the contents of a given block in several formats and the details of an inode, including all the block numbers. TCTUTILs is tested on OpenBSD, Linux and Solaris.

Autopsy Forensic Browser is an HTML based front-end interface to TCT and TCTUTILs. It allows an investigator to browse forensic images generated from a file, inode or block level abstraction. It also provides a convenient interface for searching for key words on an image. It browses a forensic image from the file/directory level using a File Manager style interface, searches the image at the block level for specified strings and displays the file contents in raw, ASCII, or hexdump. Finally, it generates autopsy reports on files, blocks or inodes with their MD5 hash values.

Lazarus is another program in TCT. Its goal is to give unstructured data some form that can be viewed and manipulated by the examiner. It achieves this goal via a few simple heuristics. It begins by reading in a block of data from its input stream and roughly determining what sort of data—text or binary—the block is. This is done by examining the first ten percent of the bytes in the block—if they are mostly unprintable characters, then it is flagged as a binary block; otherwise, it is flagged as text data. If the block has been flagged as text, Lazarus checks the data against a set of regular expressions to attempt to determine what it is with finer detail. If the block is binary, the Unix file command is run over the chunk of data to classify the file based on its content. If the data block is not specifically recognized after the initial text/binary recognition but instead follows a recognized chunk of text/binary data (respectively), Lazarus assumes that it is a continuation of the previous data and will concatenate it to the previous data block. These discrete files are then individually written to disk.

2. Computer Incident Response Suite
from New Technologies, Inc
www.secure-data.com/suite1.html

CRCMd5 is a CRC program that mathematically creates a unique signature for the contents of one, multiple or all files on a given storage device. Such signatures can be used to identify whether or not the contents of one or more computer files have changed. This forensics tool relies upon 128-bit accuracy and can easily be run from a floppy diskette to benchmark the files on a specific storage device. CRCMd5 can be used as the first step in the implementation of a configuration management policy. Such a policy and related system bench marking can help computer specialists isolate problems and deal with computer incidents after they occur. The program is also used to document that computer evidence has not been altered or modified during computer evidence processing.

DiskScrub is a scrub utility used to eliminate data on the hard disk drive. The data storage areas are repeatedly overwritten in such a way that the original data cannot be recovered using data recovery or computer forensics software. This process involves writing data on the hard disk drive tracks from the first sector to the last sector on the subject hard disk drive. DiskScrub conforms to US DoD computer security standards, which require that the data overwrite process involve one pass with a character, a second overwrite pass using the compliment of the first character overwrite and a third pass with a random character.

DiskSig is another CRC program that validates mirror image backup accuracy. This program is used to mathematically create a unique signature for the content of a computer hard disk drive. Such signatures can then be used to validate the accuracy of forensic bit stream image backups of computer hard disk drives. This program was primarily created for use with SafeBack software.

FileList is a disk catalog tool used to evaluate computer use time lines. It documents information about files stored on one or more computer hard disk drives and other computer storage devices. This multi-purpose tool is designed for covert use, security reviews and forensic laboratory processing of computer evidence. It leaves no trace that it has been used and the output is compressed so that the output will usually fit on just one floppy diskette. The compressed output is automatically converted into a dBASE III file format by a companion program FileCNVT. The dBASE III file format will import into most commercial spreadsheet and database applications. The converted output can also be viewed, sorted and analyzed through the use of timeline analysis tool ShowFile. FileList is compatible with DOS, Windows, Windows 95/98 and a special version is available for Windows NT systems. The Windows NT version is sold separately.

Filter I is an intelligent fuzzy logic filter for use with ambient data. This enhanced forensic filter can quickly make sense in the analysis of Windows swap file data, file slack data and data associated with erased files. It relies upon pre-programmed artificial intelligence to identify fragments of word processing communications, fragments of E-mail communications, fragments of Internet chat room communications, fragments of Internet news group posts, encryption passwords, network passwords, network logons, database entries, credit card numbers, social security numbers and the first and last names of individuals that have been listed in communications involving the subject computer. This unique computer forensic tool can also be effectively used in computer security reviews as it quickly reveals security leakage and violations of corporate policy that might not be uncovered otherwise. The software does not rely upon key words entered by the computer specialist. It is a pattern recognition tool that recognizes patters of text, letter combinations, number patterns, potential passwords, potential network logons and the names of individuals.

GetFree is an ambient data collection tool used to capture unallocated data. It is used to capture all of the unallocated file space on DOS and Windows 95/98 systems. It can be used to validate the secure scrubbing of unallocated storage space with the M-Sweep ambient data deletion software. When used as an investigative tool, it eliminates the need to restore files on the hard disk drives. GetFree has also proven to be an ideal tool for use in computer security risk assessments because the software automatically captures the data associated with unallocated file space. This tool is ideal for the validation of the results when computer security scrubbers have been used. Thus, it aids in the process of security certifications of computer storage media.

GetSlack is an ambient data collection tool used to capture file slack. It is an ideal computer forensics tool for use in investigations because memory dumps in file slack are the cause for security related concerns. Typically, network logons and passwords are found in file slack. It is also possible for passwords used in file encryption to be stored as memory dumps in file slack. From an investigative standpoint, file slack can contain leads and evidence in the form of fragments of word processing communications, Internet E-mail communications, Internet chat room communications, Internet news group communications and Internet browsing activity. It also acts as a good validation tool for use with computer security programs designed to eliminate file slack

GetTime is used to document the system date and system time settings of the subject computer. File dates and times associated with allocated files and previously deleted files can be important in cases involving computer evidence. The reliability of the file dates and times are directly tied to the accuracy of the system settings for date and time on the subject computer. It

is thus important to document the accuracy of the system clock.

Net Threat Analyzer is a forensic internet analysis software used to identify corporate internet account abuses. The software relies upon computer artificial intelligence logic to quickly identify patterns of computer data tied to Internet E-mail communications, Internet Browsing activity and the download of files from Internet sites. It is used to identify Internet activities that have been transparently stored in ambient data storage areas of computer hard disk drive, to evaluate Windows swap files and investigative leads in the form of file slack and unallocated data storage areas.

M-Sweep Pro is an ambient data security scrubbing utility for use on notebook computers that contain sensitive computer data. It also has application both with desktop computers and in the safe exchange of data via floppy diskettes and Iomega Zip Disks. This software repeatedly overwrites data storage areas. It is compatible with DOS, Windows 95/98/NT/2000. It meets US government requirements for the secure deletion of computer data and it deals with threats associated with shadow data concepts.

NTI-Doc is a documentation program for use in recording file dates, times and attributes. This program is used to essentially take an electronic snapshot of files and subdirectories that have previously been identified as having evidentiary value. The program automatically creates documentation that can be printed, viewed or pasted into investigative computer forensic reports.

PTable is a utility used to review and analyze the partition tables assigned to a hard disk drive. This tool is essential concerning network forensics or when multiple operating systems are stored on one hard disk drive in multiple partitions. It can also used to identify hidden data potentially stored in the partition gap or unknown partitions.

Seized is a program used to lock and secure evidence computers. It limits access to computers that have been seized as evidence. When the program is operated, it locks the computer system and displays a message on the screen advising the computer user that the computer contains evidence and it should not be operated without authorization. The program is to be installed on a DOS system diskette for placement in the floppy diskette drive on the computer system and is to be called from an AUTOEXEC.BAT file. Once the program has been called it, locks the computer and displays the warning message on the screen.

ShowFL is a program used to analyze the output of file list. It is intended for use with the FileList software. It allows for easy sorting, analysis and viewing of database output.

TextSearch Plus is a text search utility used to locate key strings of text and

graphic files. It quickly searches hard disk drives, zip disks and floppy diskettes for key words or specific patterns of text. It operates at either a logical or physical level at the option of the user. It is compatible with FAT 12, FAT 16 and FAT 32 DOS based systems on DOS and Windows95/98.

3. EnCase
from Guidance Software, Inc.
www.encase.com/html/forensic_software.html

EnCase is the industry leading computer forensic software tool used by most all computer forensic examiners. Award winning and court tested, EnCase software allows law enforcement and IT professionals to conduct a powerful, yet completely non-invasive computer forensic investigation. EnCase features a graphical user interface that enables examiners to easily manage large volumes of computer evidence and view all relevant files, including "deleted" files, file slack and unallocated data. The integrated functionality of EnCase allows the examiner to perform all functions of the computer forensic investigation process, from the initial "previewing" of a target drive, the acquisition of the evidentiary images, the search and recovery of the data and the final reporting of findings, all within the same application. Further, EnCase methodology allows the examiner to perform these processes in a non-invasive manner, meaning not one byte of data is changed on the original evidence. The final reports and extracts generated by the built-in report feature documents the investigation results and integrity of the original data with a clear and concise chain of custody to ensure the authentication of the examined electronic evidence in a court of law.

4. Extractor
from WetStone Technologies, Inc
www.wetstonetech.com/extract.htm

Extractor is a Linux RedHat deleted file recovery tool. It can assist law enforcement, government and commercial organizations in retrieving maliciously or accidentally deleted files within the increasingly popular Linux operating system environment. The technology was initially invented to assist the New York State Police Forensic Investigation Center (FIC) with the extraction of deleted data from a Linux RedHat computer system taken as evidence on a case. The tool can extract the deleted file contents, the original file attributes, the time and date of deletion, last modification, access and creation date of the file, and the owner and group the file was a member of.

5. Forensic Recovery of Evidence Device
from Digital Intelligence, Inc.
www.digitalintel.com/fred.htm

The Forensic Recovery of Evidence Device (FRED) is a highly integrated

platform for the acquisition and analysis of computer-based evidence. FRED contains a suite of forensic software like DriveSpy, Image, PDWipe, PDBlock, PART

DriveSpy is a forensic DOS shell. It is designed to emulate and extend the capabilities of DOS to meet forensic needs. Whenever appropriate DriveSpy will use familiar DOS commands to navigate the system under investigation. When beneficial, DriveSpy will extend the capabilities of the associated DOS commands, or add new commands as necessary. DriveSpy provides a familiar DOS-like prompt during system navigation. DriveSpy does not use drive letters in the prompt, but rather a Drive/Part combination to eliminate confusion in the event where the resident operating system has not assigned a drive letter to the drive being processed.

Image is a standalone utility to generate physical images of floppy disks. The files generated by Image contain complete physical images of the diskette being processed. Image is capable of generating either highly compressed or flat images for forensic analysis. It utilizes internally implemented algorithms which are identical to those used in ZIP compatible archives. Non-compressed flat images may also be generated to facilitate examination of the image file itself. Image supports cyclic imaging and restoration to automate the processing of large numbers of diskettes. The program also provides the ability to attach descriptive information to each image file. Technical and descriptive information associated with each file may be displayed without having to actually restore the image. Image maintains an MD5 checksum of each image file it creates. This checksum compared during restoration to ensure that no degradation or corruption of the image file has occurred. Image will generate self-restoring image executables for distribution and usage without the utility itself. Image is very simple to use. Command line parameters are minimal and very intuitive.

PDWipe (Physical Drive Wipe) is a standalone utility to wipe (zero) an entire physical hard drives. It provides the option of using a character other than 0x00 when wiping a drive. It also offers the ability to wipe the drive using a random pattern. It will optionally record Logical Sector Addresses, and CHS addresses for both Int13 and Int13x geometries at the beginning of sectors as they are wiped. The latter is useful when diagnosing architectural discrepancies when moving a drive between systems or validating imaging utilities. It can also verify that the contents of a specified number of randomly chosen sectors have been wiped. If a wipe-verification is requested, it will also automatically verify the first and last sector on the drive. Command line options are provided such that the program may run from within a batch file to wipe large numbers of hard drives prior to redistribution.

PDBlock (Physical Drive Blocker) is a standalone utility designed to prevent unexpected writes to a physical disk drive. When PDBlock is executed on a

computer its job is to prevent all writes to the physical drives.

PART is a Partition Manager, which lists summary information about all the partitions on a hard disk, switch bootable partitions, and even hide and unhide DOS partitions. The PART utility adds 10x to the DOS partition type code to hide and unhide partitions. The PART utility may be used to switch between multiple bootable primary partitions.

6. Forensic Utilities
from Key Computer Service, Inc
www.cftco.com/utilities.htm

Wiper is a forensic disk wiping utility that will completely erase all information on a logical or physical drive by overwriting each and every byte with a character that is user selectable. The program is written entirely in assembly language and therefore is small and fast. It uses the BIOS disk services, even for the logical drives, thus will wipe a drive regardless of the operating system format. The user may select a one-pass wipe, using the default character of 00 or a character entered by the user, or a "secure", seven-pass wipe. The "secure" wipe uses alternating ones and zeros for six passes, then finishes the process with a pass using the user-selected character or zero, leaving a completely blank drive, except for the low level formatting information. The speed is about 3 to 4 minutes per GB per pass for a hard drive.

ListDrv is an assembly language utility that examines a logical drive, or several logical drives on a physical drive, for FAT12, FAT16, or FAT32 files. As they are found, they are saved to a comma-delimited and quotation mark-delimited file prepared for importation into a database program or a spreadsheet program such as Excel, for any desired manipulation. ListDrv will also list deleted files if desired. The listing includes the complete path, the long file name, if present, the alias or short file name, and the other date, time, size, and location information. If removable media is used to save the listing file, ListDrv will span multiple disks.

ChkSum is an assembly language disk utility that calculates a 64-bit checksum for a physical or logical disk drive.

FreeSecs is an assembly language disk utility that searches a specified logical drive for the unallocated or free space, and saves the information contained in unallocated space to one or more files. FreeSecs can additionally search any physical drive (regardless of the operating system) and save all the information contained on all sectors to one or more files.

DiskDupe is an assembly language utility that makes exact forensic copies of floppy diskettes.

DataSniffer is an excellent parsing and carving utility that can “carves" data or files from files or unused space. DataSniffer has a number of separate functions such as a file extraction utility, a data parsing utility, a image compiler utility, a recycle bin history utility and a file signature generator utility.

7. Forensic Utility Suite
from LC Technology International, Inc
www.lc-tech.com/forensicsuite.asp

The Forensic Utility Suite allows forensic recovery of data on all Microsoft operating systems. The suite is a compilation of the RecoverNT, Recover98 EXPRESS and FILERECOVERY for Windows. All of these utilities are unique in their own way providing multiple recovery options on IBM compatible Intel based computers with Windows 95/98/Me/NT/2000/XP. It is a total solution for all Microsoft file systems, allowing for fast, safe, and reliable file recovery with the ease of use of the Windows environment. The Forensic Suite comes with remote clients to do recovery across a network as well as a DOS client that allows user to recover through DOS on un-bootable machines.

RecoverNT runs natively under the Windows 95/98/Me/NT/2000/XP operating system and supports multi-boot, striped, spanned and mirrored drives as well as all versions of RAID. RecoverNT can scan and recover files that have been destroyed. It is compatible with FAT12, 16, 32 and NTFS file systems and IDE/ATA, SCSI, RAID and removable media.

Recover98 Express is a fast Undelete for Windows 95/98 with FAT File Systems. It allows the retrieval of files which have been deleted from a disk and recycle bin. It uses a unique Virtual File System that displays only deleted files and directories making finding files a simple task. The user can scan a drive and the Explorer-like interface displays the recoverable files.

FileRecovery for Windows is a cross platform undelete for Windows 95/98/Me/NT/2000/XP. It supports FAT12, FAT16, FAT32 and NTFS formats. The new Search and Filter options make recovering files fast and easy with full preservation of the directory structure.

8. ForensiX
from Fred Cohen & Associates
www.all.net/

ForensiX is a software embedded in a system, using a wide variety of existing tools to aid in forensic analysis of digital evidence. This comprehensive digital forensic analysis package images and analyzes Mac,

DOS, Windows, Unix, and other disks and files, PCMCIA cards, IDE, SCSI, parallel, serial, IP traffic and other data sources. It searches for known site names and known digital fingerprints. It automatically produces chain-of-evidence information to assure the integrity of the imaged data, generate reproducible analytical results and documents the analysis process.

9. Omniquad Detective
from Tech Assist, Inc
www.toolsthatwork.com/ttw-tools.shtml

Byte Back is a professional data recovery and computer investigative utility with powerful low level cloning, imaging, and disk analysis tools. It clones and images most drive formats, repairs Partitions and Boot Records of FAT12, FAT16, FAT32 and NTFS volumes, offers individual file recovery for these environments, quickly overwrites every sector of a drive, contains a powerful sector editor for working with raw data and performs an in-depth read-only scan of a disk's surface. It supports drives up to 4 terabytes, archives images and reports to most network storage devices and perform safe recoveries on hard disk, Zip, Jaz and floppy. It has the ability to search for any character string on the entire drive, including slack areas, and gives on-the-fly direct control over the system's Read Retries, Process Delay and Timeout. It is also integrated with MD5.

Desktop Surveillance is a combination of a Network Intelligence Management and Productivity tool and a Desktop Content Security utility. It can identify every action performed by the user and record those actions in three different ways: virtual video, keystroke capture and smart activity logging. It monitor and records all Windows desktop activity, such as keystrokes, e-mail, chat, surfing, instant messaging and hacking with powerful access control and filter capabilities. The monitor can operates in a Prevention mode to make the users aware that their actions may be monitored or in the Stealth mode without the users' knowledge. Desktop Surveillance can be remotely controlled via local network or the Internet, and in both cases it is possible to remotely observe activity on the local desktop in real-time. Its access control provides an ability to easily design, create and implement an organization-wide acceptable usage policy to launch Blocking, Limited Access or Lockdown functions.

Detective is a software tool designed to allow for rapid investigation of the contents and activities of a Windows PC. It investigate the history of the PC to determine what the system was used for, such as which web sites were visited, what images were downloaded. Detective can be installed on the file server and operated in batch mode. This will simultaneously scan network workstations and save results on the network server for easy retrieval by the system administrator. It can also automatically perform the scan according to preset parameters, providing either a separate report for each workstation or

only one summary log to be appended each day.

10. Ultimate Toolkit for the Forensics Specialist
from AccessData Corporation
www.accessdata.com/products.htm#Modules

Password Recovery is a toolkit that handles all password recovery needs in one package, with a wide variety of individual password breaking modules.

NT and Novell Password Replacement Utilities allow continued access to Windows NT and Novell file servers with replacement of administrator password.

Distributed Network Attack (DNA) is a utility for recovering password-protected files. DNA decrypts password protected Microsoft Word and Excel, and Adobe Acrobat (PDF) documents, using an exhaustive key search. The DNA Manager is installed in a central location where machines running DNA Client can access it over the network. DNA Manager coordinates the attack, assigning small portions of the key search to machines distributed throughout the network. DNA Client will run in the background, only taking unused processor time. Users will see no difference in processor speed since DNA Client cannot override a higher priority program. The program uses the combined processing capabilities of all the attached clients to perform an exhaustive key search on Office 97/2000 encrypted documents to decrypt the file.

Forensic Toolkit (FTK) is a handy utility for computer crimes investigators. FTK offers users a complete suite of technologies needed when performing forensic examinations of computer systems. Its full text indexing offers quick advanced searching capabilities. In addition, the FTK has incorporated Stellent's Outside In Viewer Technology to access over 255 different file formats. The Known File Filter (KFF) feature can be used to automatically pull out benign files that are known not to contain any potential evidence and flags known problem files for the investigator to immediately examine.

SecureClean provides reliable and comprehensive protection to electronically shred information by purging deleted files on the PC. It also cleans cache, cookie and history files from IE4 and IE5 in real time.

CleanDrive offers reliable and comprehensive protection to electronically wipe the hard drive. CleanDrive includes two utilities: WipeDrv and CleanDrv. WipeDrv erases data from a physical hard drive, independent of the format, including the partition tables. CleanDrv is a secure drive reformatting utility that both reformats and erases drive data stored on FAT12, FAT16, and FAT32 formatted drives. It erases filenames, folder

names, file content, the file information tables and the logical drive partitions (drive letters). Both the CleanDrive utilities support any size hard drive and can overwrite drive data 1, 3, 7, 12, or 35 times.

11. Vision
from Foundstone
www.foundstone.com/products/

Vision is a forensic utility that maps all of a host's executables to corresponding ports, allowing the examiner to identify and investigate suspicious services. It allow the interrogation of suspected services to identify backdoors and Trojan applications. If a malicious service is identified, it can immediately kill the process.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D: SUMMARY OF REQUIREMENTS OF A COMPUTER FORENSIC INVESTIGATOR

1. An investigator requires a capability to simultaneously preview a large number of systems on site to determine which ones contain relevant evidence. In most cases, an initial search at the physical level of the media may be sufficient to determine if a specific computer system or piece of media contains relevant information and should be imaged and preserved for further more detailed analysis. However, a search at the logical layer would be also required to look for relevant files that may be compressed, encrypted, encoded, or with reserved keywords that may be physically fragmented on disk.

2. An investigator requires the capability to conduct a search at the physical level of the target media, ignoring operating system and file system logical structures, regardless of the logical content. This physical search of the media essentially searches all logical files, file slack, free or unallocated space, and all space on the media outside any logical data areas.

3. The search tool must be able to reliably report the physical location on the media where responsive data were found. Even though a physical search is conducted, the search tool may be able to determine whether the keyword resides in a logical file on the media, in file slack, in free space, or in areas of the media outside the logical data area. The investigator must be able to discern the context within which a word or phrase resides on the media to determine if the context is relevant to the investigation. So the search tool must be capable of displaying some amount of data that resides on disk immediately prior to the keyword and some amount of data that resides on disk immediately after the keyword.

4. An investigator requires the capability to conduct a thorough, read only search at the logical level of the target media. A search of the logical file space is likely to require less time than a search of the physical media, but likely will not search every sector of the media. If an investigator begins with a logical search to preview media, and that search produces no relevant results, the investigator may have to follow up with a search of the physical media to ensure a thorough search.

5. An investigator requires an ability to generate a listing of all logical files in a file system. This listing must include not only all the regular files in a file system, but also all files with special attributes, such as hidden files, read-only files, system files, executable files, directories, links to files, device files, etc. And the tool that creates this list must be able to write the list of files to appropriate media, whether that is a network accessible volume, a local hard drive not under investigation, or some appropriate removable media connected to the analysis machine. In addition, an investigator requires an ability to generate a listing of all the date and time stamps an operating system may store in relation to each file in the file system. Further, an investigator requires the ability to identify and generate a listing of all deleted files in the file system. Various operating systems handle deleting files in various ways, so the specific capability of a tool will be dependant on the file system the tool is examining, but to some degree, all file systems have a way of at least identifying that a file once existed in a certain space.

6. An investigator requires an ability to search the contents of the regular files in a file system without changing either the data in the file or any date and time data recorded by the operating system about the file. Some search tools that operate at the logical level of the media do not quite meet this requirement. If a search tool allows the operating system to update date and time stamps of last accessed when the tool runs, then the investigator must take steps to preserve those date and time stamps prior to using the search tool.

7. An investigator requires an ability to identify and process special files. Special files are in a format where their contents not in a readily readable, searchable format. These include encrypted, compressed or password protected files; steganographic carrier files; graphics files, video files and audio files; PDF format files; executable files or binary data files; files housing email archives and/or active email content; swap files or virtual memory files, and other such file formats that obscure their plain text content.

8. An investigator requires the capability to recover pertinent deleted files or portions thereof that have not been overwritten. This would logically include a capability to identify and search all file slack, identify and search all free and unallocated space, identify relevant file headers in free space, identify deleted directories in free space, including directory entries for deleted files, and recover deleted directory entries as well as all pertinent deleted files that are not overwritten.

9. An investigator requires the capability to make forensically sound images of a wide variety of media. Once the preview process has identified that certain systems or media contain information relevant to the issues at hand, an investigator must have tools capable of making forensically sound images of those systems or media. The image must include a true, validated copy of every bit of every byte contained on the media, without regard to media contents.

10. An investigator requires the capability to restore forensic images to suitable media. This requirement stems from a need to be able to run applications installed on drive that have been preserved as evidence. Most applications rely on installation processes that do more than just copy the application files to the media. So running the application in its installed environment may be necessary. This cannot currently be done from within the image files, so the image must be restored.

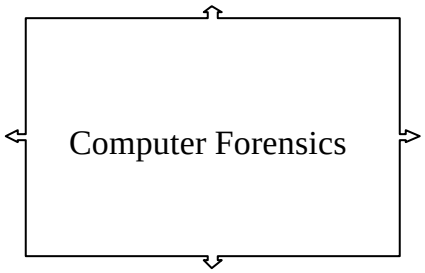
11. An investigator requires the capability to perform a sector-by-sector comparison of two pieces of media to determine where they differ. To verify that one piece of media is an identical copy of another, investigators typically use media hashes of some type. But where two pieces of media are thought to be identical copies of each other but hash differently, it must be possible to compare sector-by-sector. The tool should also verify if any of the differences between the original and the copy are merely sectors filled with 0x00 and are accounted for by geometry differences only.

12. An investigator requires the capability to thoroughly document their investigative activities and succinctly document the data recovered from a piece of media that are relevant to the allegations under investigation. If the software is self-documenting and certain reports are automatically generated for the user, based on the results of exercising the capabilities of the software, this could help make reporting results much simpler.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E: HANDOUTS FOR COURSE LECTURES

The following pages, 1 – 110, are the handouts for the course lectures.



1

Course Objectives

- To provide students with an understanding of the fundamentals of computer forensics.
- To examine how information is stored in computer systems and how it may be deliberately hidden and subverted.
- To establish a sound theoretical foundation of the methods used in extracting information for forensic examination.

2

What is Covered

- Fundamentals of computer forensics
- An overview of existing computer security mechanisms that could aid in the recovery of digital evidence for forensic analysis
- Techniques for computer evidence recovery
- Laboratory exercises on the use of common computer forensic tools

3

Reference Materials

- Handbook of Computer Crime Investigation:
  Forensic Tools & Technology
  - Eoghan Casey (editor)
- Computer Forensics Column,
  Doctor Dobb's Journal
  - Dan Farmer and Wietse Venema
- Digital Evidence and Computer Crime:
  Forensic Science, Computers, and the Internet
  - Eoghan Casey
- The Process of Network Security:
  Design and Managing a Safe Network
  - Thomas Wadlow

4

Sections

1. Cyber Crime & Incident Response
2. Introduction to Computer Forensics
3. Application of Forensic Science to Computers
4. A Structure for Forensic Investigations
5. Computer Forensic Procedures
6. Forensics using MAC Times

5

Sections

7. Forensics on Windows
8. Forensics on Unix
9. Forensics on the Networks
10. Forensics on an Unknown Program
11. Forensics on Intrusion Activities
12. Forensics on Wireless Network

6

Section 1

Cyber Crime & Incident Response

7

Cyber Crime

- Crime involving computers and networks
- Types
  - Computer as a Target
  - Computer as a Criminal Instrument
  - Computer Incidental to other Crimes
  - Crimes Associated with Prevalence of Computer

8

Cyber Crime

- Computer as a Target
  - Computer and Network Intrusion
  - Data Theft
  - Technical Vandalism
- Computer as a Criminal Instrument
  - Credit Card Fraud
  - Telecommunications Fraud

9

Cyber Crime

- Computer Incidental to other Crimes
  - Drug Trafficking
  - Money Lending
  - Child Pornography
- Crimes Associated with Prevalence of Computer
  - Copyright Violation
  - Software Piracy
  - Component Theft

10

Computer Crime

- One of the types of Cyber Crime
- Instances of Computer Crime are defined in the

US Computer Fraud and Abuse Act

11

Types of Computer Crimes

- Theft of computer services and information
- Unauthorized access to protected systems
- Software piracy
- Alterations of electronic information
- Crimes involving use of computers
- Transmission of malicious code

12

Computer Crime Prosecution

- Locate the attack areas.
- Gather adequate proof.
- Collect evidence without breaking the law.
- Select a lawyer and court familiar with the technicalities of computer crimes.

13

Computer Crime Prosecution

- Convince the court to issue an order for the appropriate law enforcement agency to act.
- Collect more evidence, ensuring that the integrity of the digital evidence is not compromised.
- Arrest and prosecute the suspect with the corroborating evidence.

14

Incident Response

- Prerequisite
  - Familiar with operations of the organization
  - Thorough understanding of the design, defenses and monitoring systems in the network
  - Aware of the system resources and tools
  - Understand the response plan for reported/detected incidents
  - Familiar with the procedures and specific tasks, and the importance of urgency

15

Incident Response

- More than often, the computer security team, the incident response team, and the computer forensic team, are the same key players wearing multiple hats.
- Some of these roles may complement each other, while others may interfere with one another.

16

Incident Response

- The tasks at hand usually compete for time and attention from these key players
  a. The incident response team needs to conduct a preliminary assessment of the compromise and tighten the security settings to minimize the damage or opportunities for repeated intrusions.

17

Incident Response

b. The computer forensic team needs to collect and preserve evidence to reconstruct the events, determine the extent of the damage, and prosecute the intruder.

c. The computer security team needs to review the computer security plan and policy to prevent recurrences of such incidents.

18

Incident Response

- It is important to be able to put aside the less important and distracting tasks that may interfere with the incident response, forensic examination or security implementation—whichever is the priority.
- This priority may change depending on the type of intrusion and incident. All key players must understand what is the priority.

19

System Discrepancies

- There are many minor discrepancies every day that are not caused by intruders.
- Too many false alarms will dull the ability of the incident response and forensic team to response properly in a real crisis.

20

System Discrepancies

- Discrepancies may not be noticed first by the incident response team but by users who are untrained in spotting computer security problems.
- The incident response team will generally exhaust many other possibilities before seriously entertaining the idea of an intruder break in.

21

React Quickly & Decisively

- You are not playing chess where there are clear rules and you can see the position of all pieces on the board.
- If you adopt a conservative plan, move and then wait for countermove, you will be playing the game the way the attacker wants it played.

22

Priorities During an Attack

1. Confirm the attack
   - Examine other information sources for confirmation to determine if the incident report is a false alarm

23

Priorities During an Attack

2. Attack Response
   - Scramble the response team
   - Determine the location of the attacker (internal or external) and means of entry, so that he can be cut off
   - Decide on a state of lockdown—monitor or halt network
   - Verify integrity of logs and logging machines
   - Estimate extent of contamination and locate contaminated systems

24

Priorities During an Attack

3. Lockdown
   - Verify integrity of essential infrastructure systems
   - Deny attacker additional access to network or attempts to switch to another machine on the network
   - Close the apparent means of entry
   - If compromise of normal shutdown procedure is suspected, pull the power cord to halt machine abruptly.

25

Priorities During an Attack

4. Stabilization
   - Ensure attacker has no further influence on the network
   - Monitor system activities to determine secondary contamination or successfully installed malicious code

26

Priorities During an Attack

5. Cleanup
   - Focus on returning network and systems to full operational status
   - Contaminated systems shall be taken offline and completely rebuilt, and watch for self- or re-infection
   - Verify that attack has not been designed to erase backup tapes when mounted

27

Priorities During an Attack

6. Restart and Monitor
   - Watch all subsequent activities from the attack source network or entries of attack

28

Investigation Checklist

- Date and time of attack or detection
- What files were compromised
  - New and hidden files
  - Unusual file or directory names and size
  - Normal-looking files out of their unusual places
    - *bin*: binary programs
    - *lib*: loaded libraries and static data files
    - *dev*: device drivers
    - *etc*: administrative programs and configuration files
    - *man*: manual pages

29

Investigation Checklist

- Which machines were compromised
  - Unusual running processes
- How initial penetration occurred
- What holes have been added
- Anomalies in logs
- Anomalies in network
  - Unauthorized network listeners

30

Managing the Incident Response

- Break up the investigation
  - Assign members to examine different areas concurrently
- Schedule regular team briefing
  - Avoid constant interruption for status updates
  - Avoid uncoordinated duplication and poor correlation
- Schedule management brief
  - Provide facts and not too much unproven speculations or undue alarms

31

Managing the Risk

- Before resuming normal business operation, be reasonably confident that it will not cause a major problem or re-attacks
- Difficult to be absolutely certain
- Need to find acceptable level of risk and get back online

32

This slide is intentionally left blank

33

This slide is intentionally left blank

34

This slide is intentionally left blank

35

This slide is intentionally left blank

36

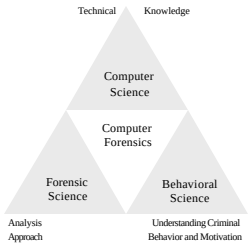
Section 2

Introduction to Computer Forensics

37

Computer Forensics

Application of scientific principles and techniques to facilitate investigation and prosecution of computer crime.



38

Requirements for Digital Detectives

- Technical awareness
- Knowing the technical implications of your actions
- Understand how data can be modified
- Clever, open-minded & devious
- Highly ethical
- Continuing education, knowledge of history
- Always use highly redundant data sources when drawing conclusions

39

Digital Evidence

- Physical Evidence in Electromagnetic form
- Pros
  - An exact copy can be duplicated to avoid risk of damaging original evidence
  - Having the right tools can help to determine if the evidence has been modified or tampered with

40

Digital Evidence

- Pros (cont)
  - Evidence may not be easily destroyed and can be recovered even when deleted
- Cons
  - Seizing, preserving and analyzing digital evidence is the greatest forensic challenge
  - Privacy concerns complicate gathering of evidence

41

Use of Digital Evidence

- Digital evidence must be preserved in its original state
- Evidence must be proven to be authentic and unaltered
- A printout or duplicate of digital evidence is admissible in court unless the authenticity of the original evidence is in question

42

US Federal Rules of Evidence

- Records of regularly conducted activity are not hearsay, and thus admissible
- Examples
  - Security logs
  - Audit logs
  - Backup

43

Collecting Digital Evidence

- What to collect?
  - Hardware
  - *All* Information Media
  - *Selected* Information Media
- Relevant when hardware or information are
  - Fruit of the Crime
  - Instruments of the Crime
  - Evidence of the Crime

44

Collecting Hardware

- Advantages
  - When hardware contains a large amount of evidence
  - Requires little technical expertise
  - Simple and less open to criticism
  - The hardware can be examined later in a controlled environment

45

Collecting Hardware

- Disadvantages
  - Risk of damaging equipment, preventing it from operating properly again
  - Risk liability for unnecessary disruption of service
  - Develop a bad reputation for a heavy-handed approach to investigation

46

Collecting All Information Media

- Advantages
  - Information and evidence can be examined later in a controlled environment
  - Working with a duplicated copy avoids damage of original evidence
  - Avoids the risk and liabilities of collecting hardware

47

Collecting All Information Media

- Disadvantages
  - Requires equipment and technical expertise
  - Risk not being able to restart computer or access entire contents
  - Risk missing evidence
  - Time consuming
  - Methods are open to criticism

48

Collecting Selected Information Media

- Advantages
  - Allow for a range of expertise
  - Able to obtain help from System Administration
  - Practical, quick and inexpensive
  - Avoid risk and liabilities of collecting hardware and information media not specified in warrant
- Disadvantages
  - May miss or destroy evidence

49

Whether to Turn the Computer Off or Leave It Running?

- Most law enforcement agencies recommend turning the computer off immediately
- Philosophy based on the assumption that evidence trail may later be erased by the intruder

50

Whether to Turn the Computer Off or Leave It Running?

- Advantages of turning the computer off immediately
  - To prevent evidence from being destroyed or corrupted
  - To contain the attack

51

Whether to Turn the Computer off or Leave It Running?

- Disadvantages of turning the computer off immediately
  - Terminate monitoring of the intruder and collection of further evidence
  - Disruption of service
  - Tip off intruder that his attack has been detected
  - Admit to hacker that he has successfully compromised the system

52

Securing Physical Evidence

- Prevent unauthorized access to powered down systems
  - Mark contaminated systems with label “Do not touch. Do not power up.”
  - Tape up power switches or remove power cords from the systems.
  - Keep contaminated systems in a secure place.

53

Reporting to Law Enforcement

- Many organizations distrust law enforcement when it comes to computer crime
- Many organizations have experienced or heard of seizure and damage of hardware and the information media as a result of severe heavy-handed approach in their investigation

54

Reporting to Law Enforcement

- These organizations will choose not to involve law enforcement until they decide it is absolutely necessary
  - which is often too late

55

This slide is intentionally left blank

56

This slide is intentionally left blank

57

This slide is intentionally left blank

58

This slide is intentionally left blank

59

This slide is intentionally left blank

60

Section 3

Application of Forensic Science to Computers

61

Application of Forensic Science to Computers

1. Recognition
2. Preservation
3. Collection
4. Documentation
5. Classification
6. Comparison
7. Individualization
8. Reconstruction

62

What is Computer Forensics?

Computer Forensics involves the identification, extraction, preservation and documentation of computer evidence stored in the form of magnetically encoded information.

63

Computer Forensics - Why?

- Many times computer evidence is created transparently by the computer's operating system and without the knowledge of the computer operator.
- Such information may actually be hidden from view and thus forensic software tools and techniques are required to preserve, identify, extract and document this computer evidence.

64

Collecting Contents from a Computer

- The computer should be shut down
- The computer should be booted using another operating system that bypass the existing one and does not change data on the hard drive

65

Collecting Contents from a Computer

- All related evidence should be taken out of RAM
- A copy of the digital evidence from the hard drive should be made

66

Bitstream Copy

- When collecting the contents of a computer memory, a bitstream copy is usually desired
- A bitstream copy duplicates everything in a cluster, including anything that is in the slack space

67

File Copy

- Unlike a bitstream copy, a regular file copy only duplicates the file and leaves the slack space behind
- The slack space or allocated space may contain important evidence

68

Evidence Collection and Preservation

- Empirical Law of Digital Evidence Collection and Preservation:
  - If you only make one copy of digital evidence, that evidence will be damaged or completely lost
- Always make multiple copies of the digital evidence

69

Evidence Collection and Preservation

- Hackers have been known to interfere with the backup process to prevent it from working correctly
  - Make certain that the copying of evidence is successful and can be accessed on another computer

70

Evidence Collection and Preservation

- It is imperative that the digital evidence is saved onto a completely clean disk or write-once media like a CD-ROM
  - Copying digital evidence on used media may allow the old data in the slack space to pollute or contaminate the digital evidence

71

Evidence Collection and Preservation

- An alternative to seizing all of the hardware or digital evidence is to just take what is needed
  - This has the advantage of being easier, faster, less expensive and less risky than shutting down a computer, rebooting it and making full bitstream copies

72

Evidence on DOS/MAC/FAT32

- Do not power off computer, RAM evidence will be lost
- To get content out of RAM, all opened programs must be closed
- When prompted to save, do not write over existing content
- Shut down the computer…

73

Evidence on DOS/MAC/FAT32

- Use a boot disk to bypass OS in the hard drive when booting up the computer
- Copy content of hard disk to clean tape, disk or CD-ROM (some I/O devices will not operate without loading specialized drivers, so have different backup devices available)
- Perform a bitstream copy

74

Evidence on NTFS

- Security partitions complicate the collection of digital evidence
- Use a boot disk to bypass the Win NT OS to access content of hard disk
- Evidence can also be collected directly by another computer connected on cable and running the disk copy utilities

75

Evidence on Unix

- Unix allows programs to run on background, hence it is necessary to explicitly list all processs using *ps –aux*
- Extract key evidence from RAM on unfamiliar or suspicious processes using *gcore*
- Booting a Unix machine off a boot disk is a complicated process, be careful to avoid destroying digital evidence
- Make a bitstream copy using *dd*

76

Documenting Digital Evidence

- To support that digital evidence is authentic, unaltered and in its original state
- Since digital copies of evidence are identical, labeling helps to tell them apart from the original
- Labeling is particularly crucial when there are several computers with identical components

77

Documenting Digital Evidence

- Labeling can support a chain of custody for the digital evidence, thus establishing complete control of the evidence at all times
- A complete list of all files, properties and message digests should be filed and properly documented

78

Message Digest

- A message digest produces a statistically unique hash for a given input and is always the same for the same input
- Examples:
  - MD 5 algorithm
  - Tripwire application

79

Message Digest

- Message digests provide statistically uniqueness of a file, hence they are sometimes referred as digital fingerprint
- A message digest of the digital evidence will produce a different hash if the digital evidence has been tampered with

80

Message Digest

- Digital signature adds authenticity to the message digest

Message Digest = Integrity
Digital Signature = Authenticity

81

Individualization of Evidence

- Comparing digital evidence with a control specimen can highlight unique aspects of the evidence
- These individualizing characteristics of the digital evidence can be used to
  - link cases
  - generate suspects
  - associate a crime with a specific computer

82

Individualization of Evidence

Richard Smith tracked down the creator of the Melissa virus based on the Ethernet address of the computer embedded in the Word97 document

83

Classifications of Digital Evidence

- By Contents
  - Using the contents of an email meassage to classify it and to determine which computer it came from
  - Swap files and slack space contain a random assortment fragments of digital data that can often be individualized

84

Classifications of Digital Evidence

- By Function
  - Examining how a program functions
  - Classifying by types of malicious operations
    - Trojan
    - Virus
    - Worms
  - Identifying the computer that remotely controls or creates the program

85

Classifications of Digital Evidence

- By Characteristics
  - Classifying the digital evidence by
    - File names
    - Message digests
    - Date stamps
    - etc

86

Forensic Computing

Gathering and analyzing data in a manner as free from distortion or bias as possible to reconstruct data or what has happened in the past on a system.

87

Digital Evidence & Reconstruction

- 2 aspects of reconstruction
  - Reconstructing digital evidence that has been damaged
  - Using digital evidence to reconstruct events surrounding the crime

88

Reconstructing Damaged Evidence

- Slack Space
  - A deleted file can often be easily recovered
  - A deleted file that is partially overwritten still leaves partial information in the slack space
  - More difficult for Unix since high level of activities quickly overwrite deleted information.

89

Reconstructing Damaged Evidence

- Shadow Data
  - Result of minor imprecision that naturally occurs when data is being written on a disk
  - Only some part of the data is over written leaving other portions untouched
  - Scanning probe microscopes and magnetic force microscope can recover these fragments to reconstruct the original evidence

90

Reconstructing Damaged Evidence

- Binary Files
  - Evidence can also be retrieved from Swap files that are used to store temporary information
    - PAGEFILE.SYS in Win NT
    - Dedicated swap partitions in Unix

91

Reconstructing A Crime

- Using digital evidence to determine actions surrounding a criminal act
- Establish what has happened, who caused the events, when, where, how and why

92

Reconstructing A Crime

3 aspects:

- Relational
  - Identifying the object, its source, and relations to other objects
- Functional
  - How the object was used
- Temporal
  - The chronological sequence of the actions and events

93

Reconstructing A Crime

- Avoid Pitfalls
  - Do not be too dependent on digital evidence. Look for supporting physical evidence when possible
  - Do not be influenced by the media, which tend to sensationalize and misreport facts, thereby changing the way we perceive facts.

94

Digital Evidence Guidelines

- Do not violate any laws or give rise to liability when collecting digital evidence
- If these laws are violated, the evidence could be inadmissible
- Obtain a search warrant if necessary
- If the seizure interrupts a business unnecessarily, the investigators could be held personally responsible

95

This slide is intentionally left blank

96

Section 4

A Structure for Forensic Investigations

97

Forensic Investigation Requirements

- Evidence preservation
- Lead formulation
- Focused searches
- Temporal analysis
- Evidence recovery

98

Collection and Preservation

- After computer equipment has been seized, the evidence it contains must be collected in a way that preserves its integrity.
- Employ an imaging utility to capture a forensically sound binary image of the evidence.

99

Collection and Preservation

- While processing an evidence disk, run a message digest program and record its output.
- Periodically, validate the entire logical file system or specific files to ensure they have not changed.

100

Collection and Preservation

- Disk-level (as opposed to logical-level) hashing is not viable because even hard drives of the same manufacture, model and lot number may differ in size and location of bad sectors and maintenance sectors.

101

Testing Initial Tools

- Trust in Forensic tools should not be explicitly based on the word of the vendor.
- Long-held beliefs that a certain tool will perform its function in a forensic manner must be tested.

102

Testing Initial Tools

- Imaging utilities must be tested thoroughly or have its source code vetted to ensure the pristine nature of evidence.
- To test a tool, take hashes before and after imaging to determine if there are any discrepancies.

103

Testing Initial Tools

- Another effective way to stress test tools is to manipulate the access modes of the controlling BIOS.
- Submit the tools to an array of size, bus and content testing, and from at least two operating systems.

104

Testing Initial Tools

- James Holley conducted a thorough test of forensic imaging utilities.
  - Numerous imaging utilities worked fine against the IDE chain.
  - This discovery awakened many users and sparked investigations of other tools.
  - see Computer Forensic Tool Testing (www.cftt.nist.gov)

105

Formulating Leads

- When dealing with child pornography, this stage might involve analyzing all URLs and extracting all images on the suspect's hard drive.
- When investigating an Intellectual Property theft, it may be sufficient to analyze communications and data transfers, and perform a key word search.

106

Formulating Leads

- The examiner must find an acceptable level of 'hits' during a search.
- In some cases, false positive during the leads generation phase can be useful.
- However, in other situations this may be impractical, overly expensive, or detrimental to the investigation.
  - Client may have expense constraints
  - Short window of opportunity
  - Non effective case management.

107

Formulating Leads

- Drawbacks of finding too little information.
  - Failure to find critical evidence can
    - Stop investigations
    - Destroy investigation confidence in the examiner

108

Formulating Leads

- Having numerous lead-generation tools is vital.
- Although buying more than 1 or 2 sets of tools can be expensive, it is a necessary aspect of computer forensics.

109

Formulating Leads

- Unix search and analysis commands are reasonably powerful.
  - *awk* is extremely powerful for performing analysis.
  - *grep* search can output binary data such as carriage returns and line feeds. This data can be piped to *awk* to redirect the requisite evidence into smaller database files.

110

Focused Search

- Search the medium for specific information.
- Focus and precisely pinpoint exactly the relevant details.
- Conduct
  - Regular expression searches
  - Shell pattern searches
  - Hexadecimal searches

111

Focused Search

- With NT being as ubiquitous as it currently is, support for Unicode is a requirement.
- If a tool does not understand Unicode, it will miss vital evidence.

112

Temporal Analysis

- Temporal analysis is performed to ascertain date and time information of the evidence.
- Identify deleted files, deleted subdirectories and when they are deleted.
  - Examine Windows Recycle Bin or Recycler entities in the respective registries.
- Build an analytical timeline based upon information from the sources.

113

Temporal Analysis

- In Unix file systems, it is possible to determine file deletion time, assuming the inodes involved have not been overwritten.
- Scattered data all rely upon one another and analysis of them as a whole.
- Navigate through deleted subdirectories on FAT and VFAT using hexadecimal editors.

114

Data/Evidence Recovery

- Once the evidentiary material is located, it can be recovered from the medium.
- Some tools include the slack space when recovering a file, others stop at the appropriate byte offset, excluding the slack.

115

Data/Evidence Recovery

- Recovering the contents of slack can be valuable if that slack contains additional evidentiary data, especially in Windows operating systems.
- If a file happens to require the original application that created it, slack at the end of a file can prevent the file from being viewed.

116

Data/Evidence Recovery

- Certain Microsoft Office applications will refuse to open a document if they detect any information past a given point.
- Other applications in Office will read only up to the offset indicated by the file's size attribute.

117

Data/Evidence Recovery

- If the application relies upon the file size to open the file, and
  - The forensic tool disturbs the file size by concatenating the slacks into an active file upon capture or recovery,
    - Trick the application into opening the file normally by modifying the file's size information.

118

Data/Evidence Recovery

- There are no tools that work against all file systems.
- Examiners should acquire file/data recovery tools capable of working against at least the top 5 most frequently used file systems
  - FAT, VFAT, NTFS, EXT2, UFS

119

Data/Evidence Recovery

- Data recovery/collection forensic tools should have error handling.
- It should log any data recovery failures.
- If it simply quits or skips the file, it is of little help.

120

Characterizing an Intrusion

- Individualization
  - Determines unique factors presented in case.
- Comparison
  - Attempts to link the 'fingerprint' of the case with other known cases.

121

Characterizing an Intrusion

- Individualization and comparison can help to link a case with other similar cases and uncover evidence that may be previously overlooked.
- Hash values for malicious files and user names that are identical to those recorded in previous cases can be helpful in linking the case to the same intruder and his usual practices.

122

Examiner's Mindset

- It is important for the examiner to remain objectives.
- If the examiner develops a set of required actions for a case type, regardless of the appearance of guilt, the evidence should stand out on its own and point to the truth.

123

Examiner's Mindset

- If the examiner picks and chooses which action to perform as he goes along, instead of building the investigation on a solid framework, human nature may cause him to 'cut to the chase' by
  - Skipping important steps
  - Not look for certain types of evidence

124

Examiner's Mindset

- Examiners must be analytical and detailed in nature; performing tasks in a meticulous manner.
- The training and background of an examiner will be a better ally than a tool.

125

This slide is intentionally left blank

126

Section 5

Computer Forensic Procedures

127

Computer Forensic Procedures

- Gain control of the situation
  - Take decisive actions
- Stop any active problems
  - Block the source of the problem
  - Limit the damage
- Map out damage area
- Prioritize areas for investigations
- Restore systems in order of operational priority

128

Turning Off The Computer

- Information that may be lost from memory
  - Processes that were running
  - Network connections
  - Mounted file system

129

Turning Off The Computer

- Shutting down a system before collecting volatile data can result in a loss of significant evidence when
  - Dealing with systems that have several gigabytes of random access memory
  - Systems have active network connections that are of critical importance to an investigation

130

Turning Off The Computer

- An abrupt shutdown may
  - corrupt important data
  - damage hardware, preventing the system from rebooting
  - cause significant disruption and financial loss

131

Turning Off The Computer

- Retained information
  - Information on the disk in the RAM slack
  - Virtual memory in the form of swap and page files

132

Examining Retained Information

- Disk editing programs and memory inspection tools can capture the entire contents of RAM and provide information about the processes that are running on a system
  - Norton Diskedit
  - *fport* (www.foundstone.com)
  - *handleex* (www.sysinternals.com)
  - *ps* and *pulist* (Windows 2000 resource kit)
  - Coroner's Toolkit (TCT) automates the collection of volatile information from live computer system (www.porcupine.org/forensic)

133

Physical vs Logical Examination

- Viewing the file logically enables the examiner to determine the type of data stored (text file, executable file, bitmap…).
- Searching at the physical level may has potential pitfalls. If a file is fragmented, with portions in non-adjacent clusters, keyword searches may give inaccurate results.

134

Challenges of Investigating Criminal Activity

- The distributed nature of networks results in a distribution of the crime scene which can create practical and jurisdictional problems.
- Digital data is easily deleted or changed, hence it is necessary to collect and preserve it as quickly as possible.

135

Challenges of Investigating Criminal Activity

- A wide range of technical expertise is required when networks are involved in a crime. Every network is different, combining different technologies in unique ways.
- A great volume of data maybe involved. Searching for useful evidence can be like looking for a needle in a haystack.

136

Challenges of Investigating Criminal Activity

- Necessary to associate an individual with specific activity on a computer or network.
- Even when offenders make no effort to conceal their identity, they can claim that they were not responsible.

137

Challenges of Investigating Criminal Activity

- Encryption can make it difficult or impossible for examiners to analyze evidence.
- Steganography, combines encryption and data hiding to create a file system that makes digital evidence recovery and reconstruction very difficult.

138

Computer Forensic: An Art or A Science?

- Because every investigation is different, it is difficult to create standard operating procedures to cover every aspect of in-depth forensic analysis of digital evidence.
- Therefore, it is important to have a methodical approach to organizing and analyzing the large amounts of data typical of computers and networks.

139

Problems Gaining Access to Data

- Difficulties of finding where the data is stored
  - Records stored off-site raise difficulties because they are not in the producing party's immediate custody.
  - The producing party may, therefore, not even know that the records exist.

140

Problems Gaining Access to Data

- Difficulties posed by Encryption
  - Encryption applications can make records impossible to recover if they are used correctly and no data recovery procedures are in place.
  - If the user forgets the password or leaves the company, the producing party may not be able to produce a readable version of a protected file.

141

Problems Gaining Access to Data

- Provision for Data Recovery
  - PGP can be configured to include Additional Decryption Key (ADK) that enables an authorized entity to decrypt and recover data.
  - Windows 2000's Encrypted File System allows for data recovery agents.

142

Problems Gaining Access to Data

- Difficulties posed by Obsolete or Missing Hardware and Software
  - As organizations upgrade, change systems and vendors, they leave a legacy of data potentially incompatible with their current hardware and software.

143

Problems Gaining Access to Data

- Difficulties posed by Obsolete or Missing Hardware and Software
  - Old file formats become incompatible with the new applications, new hardware cannot read the old media.
  - Obsolete data may require substantial time and expense to retrieve and make readable.

144

Problems Gaining Access to Data

- Difficulties posed by Obsolete or Missing Hardware and Software
  - Anticipating such a burden can mitigate its impact by
    - seeking orders or stipulations to apportion cost
    - lengthen the time to response
    - limit necessary effort on data discovery

145

Consider the Cost of Failure

- Investigation can be invasive, disruptive, and expensive.
- Evidence corruption can occur unintentionally.
- The normal use of computers and management of IT systems can result in the inadvertent destruction of evidence.

146

Preservation

- Carry out preservation procedures immediately.
- Prioritized preservation effort.
- Exercise care to preserve records and avoid possible corruption.

147

Preserve Media rather than Files

- Preserve the media, as opposed to preserving only the files that appear to be interesting at the time of initial review.
- This will help to preserve not only the files of interest but also any files that may later turn out to be important as the case progresses.

148

Preserve Media rather than Files

- Preserving the media also preserves residual or deleted data.
- The preserved media may contain other data that an examiner can use to authenticate, corroborate, dissect or discredit other files contained on the media.

149

Examining the Bits

- To reconstruct the past events with as little distortion or bias as possible.
- There are a lot of places in the system that work together when a command is executed and these places can be of forensic interest.

150

Logging Information

- Operating systems maintain records of logins and logouts, and commands executed
- Individual subsystems maintain their own logging
- Mail delivery software maintains a record of delivery attempts
- Privileged commands, such as *su* (switch *userid*), are logged for every invocation regardless of its success or failure

151

Opportunities for Tampering

- Media
  - Stash data in slack space, bad blocks.
- Firmware
  - CPU, BIOS, pal, disk, network controllers.
- Kernel
  - Loadable modules, on-the-fly memory patches.
- Applications
  - Rootkit trojan horse system utilities

152

Opportunities for Tampering

- Library software
  - Execute trojan, open good file, backdoors.
- Processes
  - On-the-fly memory patches.
- Time Synchronization
  - NTP sync corrupted between network and logging devices.

153

Layers of Information

- Raw bits
  - Media, RAM, wiring, buses
- CPU Controllers
  - Memory, disk, network, terminal, disk blocks, memory pages, network packets
- Kernel
  - Translates bits into files, processes, connections, sessions, authentication
- Library Software
  - Building blocks for applications
- Applications
  - Depend on both program and data files, names, files, ownership, time stamps
- Processes
  - Information processed multiple times

154

<<< Level of Information

Level of Trust >>>

Hierarchy of Trust

- Hardware
- Controllers
- Kernel
- Device drivers
- Dynamic libraries
- Commands
- The shell & environment variables

155

Correlating Information

- Each individual log file gives its own limited view of what happened on a system
- How trustworthy is information from that log file when an intruder had an opportunity to tamper with the record to cover his tracks
- Multiple sources of information must be correlated to reconstruct events

156

Understanding Data Storage

- File systems typically store files as contiguous sequences of bytes, organized within a directory hierarchy
- Files and directories have attributes that are stored separately
- Deleting a file from the file system generally does not destroy its contents or attributes

157

Understanding Data Storage

- Traces of older magnetic patterns still exist on the physical media
- Destroying or modifying data to hide evidence can leave significant marks

158

Logical Abstractions

- The trustworthiness of information is determined by its logical layering
- Only the physical level within the magnetic domains is real, however it is also the least accessible
- Abstractions of disk blocks, contiguous files and directory hierarchies are created by software which may have been tampered with

159

Logical Abstractions

- The more levels of abstraction, the more opportunities for mistakes
- Without a file system, disk blocks are no longer grouped together into meaningful objects - reconstruction can be like solving a puzzle
- With more layers of abstraction, information becomes more ambiguous

160

Logical Abstractions

- Stored information can be volatile and persistent at the same time
- The volatility of stored information is largely due to the abstractions that make the information meaningful

161

Order of Volatility

- Registers, peripheral memory, caches
- Memory (kernel, physical)
- Network state
- Running processes
- Disk
- Floppies, backup media, etc.
- CD-ROMs, printouts, etc.

162

Preventing Harm to the Business

- Taking hard drives from computers has a tendency to stop productivity.
- A quick solution would be to copy the hard drives so that the copy could be put in service and the original held for review.

163

Evidentiary Images

- To obtain copies of the media for evidence, forensic analysis, or data recovery purposes, the producing party should make either an *exact bit for bit copy of each medium.*
- Theses evidentiary images (or duplicates) are to be used in the subsequent examinations or data recovery efforts instead of the original media.

164

Evidentiary Images

- Bit for bit copying captures all the data on the copied media including hidden and residual information. Residual data permits the examiner to reconstruct deleted files.
- Preserving the media in bit for bit copies, as opposed to just copies of files, allows the flexibility to delve into facts and details the files themselves cannot disclose.

165

Evidentiary Images

- When the media can be write-protected, imaging may sometimes be dispensed with.
- The physical write protection of such media must permit the examiner to review, analyze or exact data without altering the media in any way.

166

Preparing Evidentiary Images

- Imaging process should not alter the original evidence in any ways.
- Ensure that none of the imaging processes write any data to the original medium.
- The image or duplicate should recreate the original exactly.

167

Preparing Evidentiary Images

- Note the serial number and other unique identification information of the original media, as well as the computer from which it came.
- This information permits link to its original medium and computer for authentication and identification purposes.

168

Preparing Evidentiary Images

- The difference between the computer system's time and date and the actual time and data is important to either corroborate or discount the dates and times of files on that computer.
- Record the examiner's name and the date the image was made.

169

Preparing Evidentiary Images

- The examiner's name and the date the image was made, serves as the link in the chain of custody for the evidentiary duplicate or image files.
- Maintaining a chain of custody allows the examiner to later testify as to the veracity or authenticity of particular records.

170

Imaging Procedure

1. Create an Evidence Acquisition Boot Disk (EABD) for the imaging platform.
2. Remove the hard drive(s) from the source computer.
3. Fill out an evidence tag with the serial number and other identification information.

171

Imaging Procedure

4. Label a forensically clean hard drive with an evidence label and attach the drive to the computer that will be used to prepare the evidentiary images.
5. Boot the imaging platform with an EABD. Partition and format the hard drive. This is the drive that will receive the evidence files ("Target Drive")

172

Imaging Procedure

6. Attach hard drive to be imaged ("Source Drive") to the imaging platform.
7. Load the imaging software.
8. When specifying the source and target drive, note that fdisk numbers physical drives starting at 1. The imaging software and other partition utilities may start the number sequence at 0.

173

Imaging Procedure

9. Monitoring the acquisition. Someone should attend the imaging to ensure that the acquisition completes properly.
10. Boot the original computer with a bootable floppy. Enter the commands for date and time and note on the evidence tag the data and time represented by the computer and the actual data and time.

174

Processing Electronic Records

- Three goals in filtering
  - To facilitate the attorney's review of the records by making the records readable
  - To reduce the data that the attorney's must review
  - To gather information about the records that can be used later to identify and organize the records.

175

Filtering Process

- The filtering procedure may require a workspace twice as large as the volume of data to be processed.
- Create work directories to contain
  - \prep Files requiring further processing
  - \review Data ready to be indexed for attorney review

176

Filtering Process

- Other subdirectories
  - \special Recovered, encrypted & email source files
  - \pslack Extracted slack
  - \pcluster Extracted unassigned clusters
  - \rfiles Unprocessed files after reduction
  - \rslack Reduced slack
  - \rcluster Reduced unassigned cluster
  - \converted Processed files

177

Data Filtering Steps

1. Access evidentiary image files and restore any backup data.
2. Generate file lists containing hash values.
3. Recover deleted data.
4. Recover slack and unassigned clusters.
5. Identify and remove known files.

178

Data Filtering Steps

6. Remove other unnecessary file types.
7. Remove duplicates.
8. Identify and decrypt encrypted files.
9. Extract e-mail and attachments.
10. Index text data.

179

Access or Restore Images or Backup Tapes

- Using Forensic Tools
  - Encase (www.encase.com)
  - FTK (www.accessdata.com)
  - Copy the image files to the workspace rather than using the original evidentiary images throughout the filtering process.

180

Access or Restore Images or Backup Tapes

- Backup software should contain error-checking features to verify the quality of the restored data.
- The restored files will not have the evidentiary fragility of files restored from evidentiary images, since the backup and restore operations will not have preserved residual data.

181

Access or Restore Images or Backup Tapes

- Using Backup Tools
  - Safeback (www.secure-data.com)
  - Restore hard drives from evidentiary images.

182

Access or Restore Images or Backup Tapes

- In contrast with the relative ease of restoring hard drives, restoring backup tapes can involve a substantial effort.
- The most difficult work involved in restoring backup tapes may be configuring a system that can properly receive the data.
- Data backed up off network servers often will not restore properly unless the data are restored to a system configured substantially the same as the original system.

183

Generate File Lists and Hash Values

- Obtain a list of all the files and their respective hash values.
- Since the data and time stamps of the files will change during the filtering process, the preliminary file information and hash values will serve as a reference for later checking of the authenticity or veracity of the files.
- Capture this information before any other activity might alter it!

184

File List Information

1. Long and short file names
2. Extensions
3. Last written or modified dates and times
4. Created dates and times
5. Last access dates and times
6. Logical sizes
7. File paths
8. Hash value

185

Generate File Lists and Hash Values

- Generate file lists with software tools.
- Before exporting file list, populate the file property columns with data regarding hash values, file signatures, hash sets, known file values and other significant information

186

Generate File Lists and Hash Values

- Processing of hard drive should be done in an environment that affords a level of write-protection to the data.
- However, data restored from backup tapes could be processed in Windows, since there is no concern about losing residual data such as slack or unassigned clusters.
- Software Tools:
  - *hash* and *compare* (www.maresware.com)
  - *rspsort* (www.simtel.net)

187

Recover Deleted Files

- Copy or export deleted files to the \special subdirectory
  - Use *copy* or *export* commands in Encase or FTK.
  - Preserve the directory structure in which the deleted files are found to avoid overwriting any recovered files.

188

Recover Deleted Files

- Perform data recovery work on FAT file system in DOS.
  - Lost & Found (www.powerquest.com)
- Recovery of data from other file systems will typically require the use of tools specific to those other operating system.
- To recover data from an NTFS volume, need to work within Window NT/2000
  - RecoverNT (www.lc-tech.com)

189

Recover Slack and Unassigned Clusters

- The purpose of extracting slack and unassigned clusters is to capture residual text data on the media for review
- 2 steps:
  - Extract the slack and unassigned clusters to the \pslack and \pclusters subdirectories
  - Remove non-text characters from these files and write reduced data to corresponding subdirectories in \review

190

Recover Slack and Unassigned Clusters

- Use *copy* or *export* commands in Encase or FTK.
- *getslack* and *getfree* (www.secure-data.com) extract slack and unassigned clusters from both FAT and NTFS.
- *filter_i* (www.secure-data.com), equivalent to the Unix *strings* utility, removes non-text data from the extracted material

191

Remove Known Files

- A large amount of data on the hard drive and on backup tapes consists of files, such as operating system and application files, which are not relevant to forensic investigations.
- Identifies and excludes 'known' files by their hash values.

192

Remove Known Files

- Encase or FTK have sorting and filtering features to isolate and exclude known files.
- Identify matching hash values using *compare* (www.maresware.com)
- Pipe resulting matches to *rmd* (with overwriting) or *rm* (www.maresware.com) to remove known files

193

Remove Other Unnecessary Files

- Further reduce the data set by removing files based on file types.
- File extensions do not necessarily correspond to the file type.
  - Before removing any files, first run a test to identify any files whose file type does not match its extension.
  - Compare the file's internal header information with its extension and identifies any mismatches.

194

Remove Other Unnecessary Files

- Verify file extensions versus file types
- Moves mismatched files to \special subdirectory for separate processing
- Removes remaining files of known types
- *diskcat* (www.maresware.com) identifies file extensions against mismatched file types
- *rmd* or *rm* to remove irrelevant files

195

Remove Duplicates

- Deduping
  - Remove duplicates of all data that have not changed between backup sessions.
  - Identify duplicates by matching names, path and hash values

196

Identify and Decrypt Encrypted Files

- Identify encrypted files in the remaining data and attempt to decrypt them if possible.
- Identify encrypted data by scanning files for specific character strings in file headers or footers.
  - FTK (www.accessdata.com)
  - Password Recovery Toolkit (www.accessdata.com)
  - *ispgp* (www.maresware.com) identifies PGP encryption

197

Identify and Decrypt Encrypted Files

- Moves encrypted files to \special subdirectory for decryption
- Attempt to obtain the password from the person who encrypted the file
- Otherwise, recover the password for the encrypted file with password recovery software
  - Password Recovery Kit (www.data-secure.com)

198

Extract E-mail

- Some e-mail applications store message and attachments in proprietary formats that cannot be reviewed with text-searching software. Need to rely on appropriate email application.
- Extracted e-mail messages should be converted to a text format that can be indexed for data reduction, de-duping or decryption as necessary

199

Indexing

- After data reduction, the \review directory now consists of
  - \rfiles All the files not excluded by data reduction
  - \rslack All data from slack
  - \rclusters Unassigned clusters
  - \converted Recovered deleted files, decrypted files, extracted e-mails.

200

Indexing

- Search through the files in the /review directory by running a series of string and index-based searches.
- Review the indexing log to determine if any files could not be indexed and why.

201

Indexing

- For an index-based search
  - Index the entire review directory using a search application
    - dtSearch (www.dtsearch.com)
  - Indexing will take time since search will read each file and build a database of all terms and character combinations found in each of the files.

202

Bates Numbering

- Number the records for electronic management.
- This provides a more accurate way to refer to files.
- Sequential numbering schemes are traditionally used by attorneys to label paper documents for identification.

203

Bates Numbering

- *bates_no* (www.maresware.com) generates a unique serial number for each file
- After Bates numbering, an examiner can refer to the files produced during analysis by their unique Bates number rather than file name.
- Once files have been Bates numbered, generate a new file list of all the respetive files with their hash values.

204

Section 6

Forensics using MAC Times

205

MAC Times

atime	time of last **a**ccess
mtime	time of last **m**odification
ctime	time of last status **c**hange
dtime	time of **d**eletion (Linux only)

- MAC times are volatile
- If present & unaltered, MAC times are invaluable
- Examine MAC times directly using *lstat()*

206

MAC Times

- MAC times keep track of the final time a file is disturbed
- Reading a file changes the *atime* attribute
  - When a program runs, *atime* of the executable file changes
  - Many systems can disable *atime* updates
- *mtimes* are changed by modifying a file's contents

207

MAC Times

- *ctime* keeps track of when meta information about the file has changed
- *dtime* keeps track of when the file is deleted
  - In systems without *dtime*, *ctime* may be used as an approximation of when the file was deleted

208

NTFS MAC Times

- When a file is copied, the *mtime* of the target file is the same as the original file
- The *atime* and *ctime* are the times when the new file is created
- This can make a file appear as though it was created after it was modified
- The *atime* in NTFS not always updated when a file is accessed

209

Storing File Attributes

- Unix system directories store only the names of the files and their corresponding *inode* numbers. The rest of the information about the file are kept in the actual *inode* of a file.
- NTFS relies on a Master File Table (MFT) to store information about the files in an NTFS volume.

210

Reading MAC Times

- Login from a remote host to a target system
- *inetd*
  - listens to the telnet port,
  - forks off the telnet daemon
- *telnetd*
  - executes the login program
- *login*
  - authenticates the user
  - updates the login accounting files
  - becomes the shell

211

Reading MAC Times

MAC	Permissions	File Name	See note on next slide
.a.	-rwsr-xr-x	/usr/bin/login	1
.a.	-rwsr-xr-x	/usr/etc/in.telnetd	1
.a.	-rwsr-xr-x	/usr/etc/inetd	1
.a.	-rw-r--r--	/etc/group	2
.a.	-r--r--r--	/etc/motd	2
.a.	-rw-r--r--	/etc/ttytad	2
m.c	-rw-rw-rw-	/etc/utmp	3
m.c	-rw-r--r--	/var/adm /lastlog	3
m.c	-rw-r--r--	/var/adm /wtmp	3
.a.	-rw-r--r--	/etc/passwd	2
.a.	-rwsr-xr-x	/bin/csh	1

212

Notes on MAC Times

1. Programs executed
   - *login, in.telnetd, inetd, csh*
     - *atime* changed
2. Configuration and authentication files used
   - *group, motd , ttytab , passwd*
     - *atime* changed
3. System accounting files modified
   - *utmp, lastlog, wtmp*
     - *mtime* and *ctime* changed

213

Concealed Login

MAC	Permissions	Owner	Group	File Name
.a.	lrwxrwxrwx	root	staff	/usr/bin/cc
.a.	-r--r--r--	root	staff	/usr/include/lastlog.h
.a.	-r--r--r--	root	staff	/usr/include/pwd.h
.a.	-r--r--r--	root	staff	/usr/include/stdio.h
.a.	-r--r--r--	root	staff	/usr/include/sys/ fcntlcom.h
.a.	-r--r--r--	root	staff	/usr/include/sys/file.h
.a.	-r--r--r--	root	staff	/usr/include/sys/signal.h
.a.	-r--r--r--	root	staff	/usr/include/sys/stat.h
.a.	-r--r--r--	root	staff	/usr/include/sys/ stdtypes.h
.a.	-r--r--r--	root	staff	/usr/include/sys/ sysmacros.h
.a.	-r--r--r--	root	staff	/usr/include/sys/types.h
.a.	-r--r--r--	root	staff	/usr/include/utmp.h
.a.	-r--r--r--	root	staff	/usr/include/vm/faultcode.h
.a.	-rwxr-xr-x	root	staff	/usr/lib/cpp
.a.	-rw-r--r--	bin	bin	/usr/lib/lang_info
.a.	-r-xr-xr-x	root	staff	/usr/bin/as
.a.	-r-xr-xr-x	root	staff	/usr/lib/ccom
.a.	lrwxrwxrwx	root	staff	/lib
.a.	-rwxr-xr-x	root	staff	/usr/bin/ld
.a.	-rwxr-xr-x	bin	bin	/usr/lib/compile
.a.	-rw-r--r--	root	staff	/usr/lib/crt0.o
.a.	-r-xr--r--	root	staff	/usr/lib/libc.sa.1.8

214

Concealed Login

- The *cc*, *cpp*, *as*, and *ld* commands were executed
- Several header files (lastlog.h and utmp .h) were accessed
- A C program was compiled
- System doesn't show any login activity

>> Someone probably broke into the system and compiled a stealth program to remove the presence from the system accounting files

215

MAC Times are Universal

- MAC times can be obtained from a running machine or a dead disk
- The machine reading the MAC times does not have to be of the same operating system type as the system that generated the data

216

MAC Times are Delicate

- Collect MAC times as quickly as possible before gathering any other forensic data that might destroy them
- Collecting MAC times must be done cautiously
  - *lstat()* directories before opening them and examining their contents
  - Opening a directory for reading changes the *atime*

217

MAC Times are Delicate

- Message digest must be done after the *lstat()*
  - Reading a file changes the *atime* of that file
- Work from a duplicate
  - Mount the media as read-only
  - Alternatively, turn off *atime* updates

218

MAC Times are Invaluable

- MAC times can provide invaluable information about what programs and files are used on operating system startup or shutdown
- Windowing systems in firewalls and other security-sensitive systems add tremendously to the system complexity
  - Too many file accesses, can cloud MAC times analysis
  - Operating systems that cannot operate without a windowing system have an inherent security disadvantage

219

MAC Times of a Deleted File

- When a file is removed, the *ctime* is set to the time when the last link to the file has been destroyed, which is most often at the time it was deleted
- The *inode* is also deleted from the directory entry, making recovery difficult, but not impossible

220

MAC Times of a Deleted File

- UNIX
  - Ownership and MAC times are preserved
- NTFS
  - Does not remove all the file information, it sets a flag in the file record of the MFT telling the file system that the file is not in use anymore

221

Problems with MAC Times

- MAC times only report on the last time a file has been disturbed
- No way of reporting on the historical activity of a file or directory
- They are less useful on busy multi-user systems with lots of activity

222

MAC Times Manipulation

- UNIX systems can use *touch* command to change *atime* and *mtime*.
- NTFS and UNIX filesystems can also use *utime()* system call to change *atime* and *mtime*
- NT provides *SetFileTime()* system call to change all three times at once

223

MAC Times Manipulation

- An intruder can reset the system clock and then change the *ctime*
  - Changing the system clock can cause other warning flags
- Alternately, the intruder can write directly to the *inode.*

224

This slide is intentionally left blank

225

This slide is intentionally left blank

226

This slide is intentionally left blank

227

This slide is intentionally left blank

228

Section 7

Forensics on Windows

229

Forensics on Windows

- FAT file system
  - Comprised of file allocation table and folders.
  - Uses 8-bit ASCII/ANSI character set.
- NT file system
  - Uses several *metadata* files to keep track of files and folders on a given volume.
  - Represents all character strings in 16-bit Unicode.

230

Master File Table

- MFT is a system file created during the formatting of an NTFS volume.
- There is an MFT record for every file, including an entry for itself.
- Metadata files are located in the root folder with names beginning with '$'.

231

Master File Table

- MFT records store *attributes* of files and folder, including the MAC timestamps.
- MFT records also contain a flag that indicates its allocation status.
  - If zero, the record is marked for deletion, or is unallocated.

232

Windows 2000 Metadata Files

Record	File Name	Description
0	$MFT	Master File Table (MFT)
1	$MFTMIRR	Copy of the first 16 records of the MFT
2	$LOGFILE	List of file system transactions
3	$VOLUME	Information about the volume, including NTFS version, volume names, and volume creation time.

233

Windows 2000 Metadata Files

Record	File Name	Description
4	$ATTTDEF	Table of attribute definitions
5	.	Root folder
6	$BITMAP	Bitmap representation of used and unused clusters on volume
7	$BOOT	Boot record with bootstrap loader code if the volume is bootable

234

Windows 2000 Metadata Files

Record	File Name	Description
8	$BADCLUS	List of the bad clusters in the volume
9	$SECURE	Stores security descriptors (W2K only)
10	$UPCASE	Conversion table for converting lowercase characters to matching uppercase Unicode characters
11	$EXTEND	Enables file system extensions such as volume quotas (W2K only)

235

Files and Folders

- FAT system
  - Filenames are on stored in 32 byte structure.
- NTFS
  - Filenames (*index entries* or *index allocation*) are variable in size to accommodate variable lengths.

236

Files and Folders

- When a folder contains more index entries than it can fit in its MFT record
  - Additional data are stored on disk in *index buffers*
  - Locations of these index buffers are stored in the $INDEX_ALLOCATION attribute

237

MFT Record

- For a folder
  - Header, name, etc
  - $INDEX_ROOT
  - Index entries
  - $INDEX_ALLOCATION

238

MFT Record

- For a file
  - Header
  - $FILENAME
  - $STANDARD_INFORMATION
  - $DATA
  - Attribute List
    - Resident attributes are contained within the MFT record.
    - Non-resident attributes reside in clusters on the volume.

239

Bitmap File

- The $BITMAP file keeps track of cluster usage.
  - If a cluster is used, the bit in the $BITMAP file is changed to a one.
  - When a cluster is available, the bit is zero.

240

Bitmap File

- To allocate a file
  - The $BITMAP file must be modified to reflect that the used clusters are allocated
  - An allocated MFT record must be created for the file
  - An index entry must be created for the file name in the parent folder's MFT record or index buffers
  - Cluster extent entries must be created in the file's MFT record if the file is non-resident.

241

Bitmap File

- When a file is deleted
  - Its cluster references in the $BITMAP file are changed to zero
  - The MFT record for that file is marked for deletion, its index entry is deleted. The entry below it are moved up, thereby overwriting the deleted entry
  - The file is deleted but the data are still on the hard disk, its MFT record still exists with its deletion bit set to zero

242

Bitmap File

- Recovering a deleted file
  - If the MFT record can be located, the deleted file's resident attributes cam be recovered, including its name and timestamps.
  - NTFS overwrites deleted MFT entries before creating new ones. Therefore, any deleted files recovered from an NTFS volume will have been deleted recently.
  - The MFT records are quickly overwritten but their non-resident attributes may remain on disk indefinitely and hence can be recovered.

243

Folder Entries for FAT

- When a user *renames* a file
  - A new folder entry is created in the same folder.
- When a user *moves* a file
  - The file's folder entry in the original folder is deleted
  - A new folder entry is created in the destination folder.

244

Folder Entries for FAT

- Renaming and moving a file within a volume result in the creation of folder entries that have
  - The same dates and times as the original entries
  - The same starting clusters
  - The same file sizes

245

Folder Entries for FAT

- If a file has a short file name, the information available is the
  - Last seven characters of the filename
  - Extension
  - MAC times
  - Starting cluster
  - File length
  - Status of the attribute bits
- If a file has a long file name
  - The complete file name may be available.

246

Folder Entries for FAT

- A moved file's deleted and intact folder entries have identical
  - File names
  - Creation dates
  - Modification dates
  - Starting clusters
  - File length

247

Folder Entries for FAT

- The examiner can plot the MAC times contained in all of the folder entries pertaining to a file to identify
  - The date that the file was first placed on the volume
  - The date(s) that the user modified the file
  - The most recent date that the user accessed the file
- In NTFS, examine the MFT records and index buffer

248

Folder Entries for FAT

- If a folder is deleted, its data area is not necessarily affected.
- If the deleted folder's entry still exists in the parent of the deleted folder, that entry is marked as deleted, but the entry still contains a pointer to the data area of the deleted folders.

249

Folder Entries for FAT

- To locate deleted folders
  - Search for the occurrence of a deleted file starting with the E5 hex value
  - Search for patterns that identify a folder rather than a file.
  - Examine the cluster(s) that the folder occupied to identify entries that relate to files that were located in that folder.

250

Folder Entries for FAT

- Folders on a FAT system consists of 32 byte entries. First 11 bytes contain
  - 8 bytes short name of the file or folder
  - 3 bytes extension.
- Folders also contain 2 other 32 bytes entries for
  - The folder's parent
    - First 11 bytes contain 2 dots (2E) followed by 9 spaces (20h)
  - The folder itself
    - First 11 bytes contain 1 dot (2E) followed by 10 spaces (20h)

251

Folder Entries for FAT

- Caution:
  - After a subfolder is deleted, its data could coincidentally be overwritten by a new folder's data
  - Examiners may get a false impression that they are looking at the old folder's data when they are actually looking at the new folder's data

252

Recycle Bin

- The Recycle Bin is a hidden system folder that operates in accordance with different rules than those that govern standard folders.
- The folder is named
  - Recycled in Win95/98
  - Recycler in WinNT/2K

253

Recycle Bin

- When a user deletes a file, it is moved to the Recycle Bin. This results in
  - The deletion of the file's folder entry in the folder in which the file resided
  - The creation of a new folder entry in the Recycle Bin
  - The addition of information about the file in a hidden system file, INFO, in the Recycle Bin.

254

Recycle Bin

- The deletion timestamp can be found in the INFO file.
- Each INFO file record is
  - 280 bytes in Win95/98
  - 800 bytes for WinNT/2K

255

Recycle Bin

- Every file sent to the Recycle Bin is renamed in the following format:

  D [original drive] [index no] [original extension]
- Appended to the INFO file is
  - The file's original name and path
  - Its index number in the Recycle Bin
  - Its date and time of deletion

256

Recycle Bin

- An INFO file record containing metadata relating to a particular file is often effective in confirming or refuting computer users' explanations regarding the presence or history of computer file recovered from their drivers.
  - File deleted by the operating system do not leave a record in the INFO file.
  - INFO file record indicates that a user knowingly deleted the file.

257

Recycle Bin

- If a user's explanation for the presence of a file is that it was inadvertently downloaded during Internet activity
  - The file's location when it was deleted may tend to support or refute that contention.
  - If the user deleted a particular file residing in a default download folder, or in the Temporary Internet Files, the explanation is more plausible that if the file was in My Documents.

258

Recycle Bin

- When the user empties the Recycle Bin
  - Windows deletes the files in the Recycle Bin and the INFO file.
  - The INFO file may have been deleted but a folder entry for the deleted INFO file still remains.
  - The first character of the entry is changed to E5 hex but the rest of the entry remains intact.
  - If the contents of the files are not overwritten, the records are available for examination.

259

Recycle Bin

- From the folder entry of the deleted INFO file, the examiner can decode
  - The timestamps the files were deleted
  - The locations of those files at the time they were sent to the Recycle Bin

260

Recycle Bin

- When the INFO file has been deleted and additionally the file's folder entry has been overwritten
  - The INFO file may still be intact in unallocated or slack space.
  - The examiner can search the entire driver for unique characteristics of the INFO file's contents.

261

Recycle Bin

- If the examiner identifies an INFO file record for a file and there are no indications that the file's path existed on the seized media
  - It is an indication that there may have been another piece of media attached to the computer and there may therefore be more undiscovered evidence.

262

Recycle Bin

- If the drive letter is unaccounted for
  - It is an indication that there may have been another volume attached to the computer when the file referred to by the INFO file record was deleted.

263

Shortcut Files

- Windows\Desktop folder contains shortcut (.lnk) files.
- The shortcut files contain the fully qualified paths of the files that they refer to.
- The shortcut files may provide indications about the current and previous configuration of the user's desktop.

264

Shortcut Files

- The shortcut files have folder entries that record their MAC times.
  - The examiner can compare these dates with the dates related to the application's associated files and folders.
  - This comparison may show that the shortcut was created after the installation of the program, giving rise to the possibility that the user intentionally created the shortcut and therefore knew of the existence of the application.

265

Shortcut Files

- The installation of an application may result in the creation of a shortcut in the Windows\Start Menu folder.
- The user may move that shortcut to the desktop, but this action would result in the creation of the moved-file indicators and evidence that
  - The user knew of the application's existence.
  - An application program, which is no longer present on the computers, was installed at one time.

266

Shortcut Files

- Windows\Recent folder contains shortcut files that point to data files that were opened on the computer.
- The data area of the shortcut file contains
  - The filename and fully qualified path
  - The MAC times, which provide a secondary source to track a file's history.

267

Shortcut Files

- The MAC times provide a means of connecting a volume with the volume that the operating system is running on
  - If a shortcut file refers to a target file that is located on a removable volume, the shortcut file will contain the MAC times that appear in the target file's folder entry on the removable volume.

268

Shortcut Files

- The search for shortcut files can be conducted in the
  - Allocated area of the disk
  - Unallocated area of the disk
    - The examiner may conduct a search of unallocated space for unique characteristics of the shortcut file or its contents.
  - Swap file

269

Thumbs.DB

- Viewing any graphics files thumbnails is accomplished by the creation of a hidden system file named Thumbs.DB.
- Thumbs.DB contains a copy of each graphic files in the folder in .BMP format and their modification dates.

270

Thumbs.DB

- The user may delete files from the folders, but the copies of those files in the Thumbs.DB file may not be removed.
- Examination of the Thumbs.DB file may reveal that a file once existed on the volume and its modification timestamps, even though it is no longer existent.

271

Index.DAT

- Internet Explorer caches website that a user visits, in the C:\Windows\Temporary Internet Files folder and maps filenames to the system files.
- The Index.DAT file uses as many 128-byte blocks to describe each file. The records contain
  - The URL
  - The date that the page was last modified by the server
  - The date that the URL was last accessed by the user

272

Registry Entries

- The Windows registry is a repository for the hardware and software configuration
  - On Win95/98, registry is comprised of
    - WINDOWS\SYSTEM.DAT
    - WINDOWS\USER.DAT
  - On WinNT/2K, registry is comprised of
    - several *hive* files located in %systemroot%\system32\config
    - NTUSER.DAT files related to each user account.

273

Registry Entries

- The registry stores information about many aspects of the system in cells. A cell might reveal
  - Software installed on the subject machine
  - Recently used programs and files
  - Recently accessed servers using Telenet.

274

Registry Entries

- The Registry can be viewed using
  - *regedit* on Win95/98
  - *regedt32* on WinNT/2K
  - *regdmp* utility in the Windows NT Resource Kit to list the contents of a registry key
- In WinNT/2K, each registry key has a timestamp of the most recent update to the key.

275

Printing

- Printing involves a spooling process.
- Print spooling is accomplished by creating temporary files that contain both the data to be printed and sufficient information to complete the print job.

276

Printing

- Files with extension .SHD and .SPL are created for each print job.
- The .SHD file contains information about the print job, including
  - The owner
  - The printer
  - The name of the file printed
  - The printing method (RAW or EMF).

277

Printing

- In RAW format, the .SPL file contains the data to be printed.
- In EMF format, the .SPL file in Win95/98 is different from that in WinNT/2K

278

Printing

- .SPL file in EMF format on Win95/98 contains
  - Name of the file printed
  - Printing method
  - A list of files that contain the data to be printed.
    - The files containing the data to be printed are in enhanced metafile format
    - They have names in the format of ~EMFxxxx.TMP

279

Printing

- .SPL file in EMF format on WinNT/2K contains
  - Name of the file printed
  - Printing method (EMF or RAW)
  - The data to be printed.
- The .SHD .SPL and .TMP files are deleted after the print job is completed.

280

Printing

- In a network environment
  - The .SPL and .SHD files are found on both the workstation and the servers.
  - The examiner may examine the volume for allocated and deleted .SPL, .SHD and ~EMFxxxx.TMP files.

281

Printing

- The .SPL and .SHD files contain the name of the files to be printed and its fully qualified path.
  - The existence of a file in enhanced metafile format suggests the deliberate act of printing.
    - This may indicate knowledge on the part of the user of the existence of a particular file.

282

Printing

- The path may suggest that other media containing evidence exists.
- If the original file that the user printed does not exist on the seized evidence, the file may be found in enhanced metafile format.

283

NTFS Log File

- The $LOGFILE is created during the formatting of an NTFS volume
  - To keep track of transactions
  - To enable NTFS to recover from system crashes.
    - By documenting the operations to be conducted to complete a transaction, NTFS can undo or redo transactions that are only partially completed when a system failure occurs.

284

NTFS Log File

- To delete a file
  - The $BITMAP file must be changed to show the clusters as unallocated
  - The MFT record must be marked as unallocated
  - The index entry must deleted
- These steps are recorded in the $LOGFILE so that each step in the transaction can be executed again or undone if problems arise.
  - If a crash occurs, NTFS can complete partially completed transactions.

285

NTFS Log File

- The $LOGFILE contains
  - Index entries
    - To describes filename and MAC times
  - Copy of MFT Record
    - MFT records all file information beginning with 'File' followed by a 2A hex value
  - Link files
    - Link files are preceded with the link file header
  - Index buffers
    - Index buffers are preceded with 'INDX'

286

Windows NT Event Logs

- Microsoft WinNT can be configured to log events in binary files
  - System events in *SysEvent.evt*
  - Application events in *AppEvent.evt*
  - Security events in *SecEvent.evt.*

287

Windows NT Event Logs

- System logs include events in the system's operation such as a failed or successful driver startup, an application crash or errors associated with data lost.
- Application logs are for events recorded by applications.

288

Windows NT Event Logs

- Security logs contain information such as logon and logoff events, file manipulation, and other resource access events.
- Additionally, WinXP comes with the software-based Microsoft Internet Connection Firewall that has its own log files.

289

Windows NT Event Logs

- An event log entry has 3 sections
  - Header:
    - Date, Time, Username, Computer Name, Event Id, Source, Type, Category
  - Event Description
    - Information about the event or recommended remedy
  - Additional Data
    - Optional binary data.

290

Windows NT Event Logs

- Windows NT has descriptive messages stored in the Registry and separate files.
- The Event Viewer combines and displays the information in these files, providing a convenient way to view the data.
  - Double click to bring up the Events Details windows.

291

Windows NT Event Logs

- WinNT stores descriptive messages in the Registry and various messages files.
- Copying *.evt files from one system to another for examination may result in misinterpretation.

292

Windows NT Event Logs

- When viewing event logs on a remote system.
  - The Event Viewers will read the event record data from the remote log files, but will search the registry of the local system for the corresponding event message files.

293

Extracting Event Log

1. Extract the event logs from the image files.
2. Extract all related information referred to by the EventLog registry key:
   - *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog*

294

Extracting Event Log

3. Extract the system hives file from
   - *WINNT\System32\Config*
4. Open *regedt32*, go to
   - HKEY_LOCAL_MACHINE
5. In *HKEY_LOCAL_MACHINE*, locate key
   - *CurrentControlSet* or *ControlSet00x*

295

Extracting Event Log

6. Under the *EventLog*
   - Open the Application, Security, and System sub-keys
   - Export each key as a .reg file.
   - Examine the data portion of each key for *EventMessageFile*
   - This will reveal the path and file name of the file the Event Viewer uses to display explanatory text for each event.

296

Extracting Event Log

7. Extract the required executables (.exe) or dynamic link libraries (.DLL).
8. Edit the exported *.reg files such that
   - The path in the *EventMessageFile* statement points to the location of the appropriate extracted files on the examination system.
   - The created key should state the sub-key as *CurrentControlSet* rather than *ControlSet00x*

297

Extracting Event Log

9. Import the registry keys (*.reg) into the forensic workstation's registry.
10. It may be possible to open an extracted *.evt file with the Event Viewer using the Action|Open Log File menu option

298

Extracting Event Log

- Most of the time, the Event Viewer will report that the file is corrupted and will refuse to open it.
- The log is rarely actually corrupted
- When the event logging service does not shut down cleanly, the Windows Service Control Manager does not reset several bit values that indicate the files is open and thus cannot be accessed.

299

Extracting Event Log

- The event logging service cannot be stopped while WinNT/2K is running to prevent intruders from disabling event logging.
- *WinZapper* can break the Event Log service without shutting it down, enabling an intruder to remove individual entries from Event Log files that are in use by the system.

300

Loading Logs into Event Viewer

1. Go into Services in the Control Panel
   - Disable the events logging service.
   - The event logging is disabled automatically when the system is rebooted.
2. Reboot the forensic workstation
   - Check Services to ensure that the event logging service is not on.

301

Loading Logs into Event Viewer

3. Go to the WINNT\System32\Config folder
   - Rename the *SecEvent.evt, AppEvent.evt* and *sysEvent.evt* files to something else.
4. Copy the event logs extracted from the image to the WINNT\System32\Config folder.
5. Go into Services
   - Set the event logging service to manual start.
   - Start the event logging services.

302

Loading Logs into Event Viewer

6. Open the Event Viewer to display the logs from the imaged system.
   - This will add new events to the log files stamped with the current date and time.
7. To minimize contamination, immediately generate new copies of the event logs using the Event Viewer's *save* as command.

303

Displaying Logs in Event Viewer

- Although convenient, displaying logs using the Event Viewer is not very conducive for analysis
  - Event Viewer is not integrated with other data processing tools.

304

Displaying Logs in Event Viewer

- Microsoft recommends *dumpevt* (www.systemtools.com) for dumping contents of events logs into a format suitable for spreadsheets and databases.
- Importing contents of multiple log files into a spreadsheet makes it easier to sort events chronologically and search all the logs simultaneously.

305

Displaying Logs in Event Viewer

- When adjust for daylight saving is enabled, *dumpevt* does not adjust event time correctly
  - Events are one hour off.
- Corruption of event log record may occur
  - Accidentally due to software bugs.
  - Deliberately by reporting of misleading events that impersonate other event sources.

306

Internet Information Server Logs

- IIS logs are generally located in
  - *%systemroot%\sytem32\logfiles*
- Each time a file on a Web server is accessed over the Internet, an entry is made in an *access log* file.

307

Internet Information Server Logs

- The *access log* files are in Common Log Format (CLF)
  - Remote host
  - UserID
  - Date
  - Time
  - Request
  - Status code
  - # bytes returned
  - Referring URL
  - Browser

308

Win2K IIS Log

- IIS log in Win2K differs from CLF, and has the following format:
  - IP address
  - Date and time
  - Processing time in ms
  - Bytes sent to client
  - Bytes received by server
  - Size
  - HTTP web server access/result code

309

Web Server Access Codes

- Success
  - 200 Success
  - 201 Okay Post
  - 202 Okay Processing
  - 203 Partial Information
  - 204 Okay No response

310

Web Server Access Codes

- Redirection
  - 300 Data Requested Have Moved
  - 301 Found Data Has a Temp URL
  - 302 Try Another Location
  - 303 Not Modified
  - 304 Success/Not Modified

311

Web Server Access Codes

- Client Errors
  - 400 Bad Request
  - 401 Unauthorized Access
  - 402 External Redirect Error
  - 403 Forbidden
  - 404 File Not Found

312

Web Server Access Codes

- Server Error
  - 500 Internal Error
  - 501 Method Not Implemented
  - 502 Server Overloaded
  - 503 Gateway Timeout

313

Example of IIS Unicode Exploit

1. Intruder obtains a directory listing of C:\
   - */script/../../winnt/system32/cmd.exe/c+dir+c:*
2. Removes read-only permission on *E.asp* page
   - */script/../../winnt/system32/attrib.exe/E.asp+-r*
3. Deletes *E.asp* page
   - */script/../../winnt/system32/cmd.exe/c+sel+E.asp*

314

Example of IIS Unicode Exploit

4. Uses TFTP to download a replacement *E.asp* page
   - */script/../../winnt/system32/tftp .exe/ -i+rooted.ntserver.com+get+E.asp*
5. Runs the *E.asp* page to install trojan horse
   - */script/E.asp*

315

Example of IIS Unicode Exploit

6. Removes read-only permission on *E.asp* page
   - */script/../../winnt/system32/attrib.exe/E.asp+-r*
7. Deletes *E.asp* page
   - */script/../../winnt/system32/cmd.exe/c+del+E.asp*

316

Examining IIS Logs

- It may be possible to distinguish between an automated tool probing a Web server and a human exploring a Web server by the speed and regularity at which sequential requests are made.

317

Examining IIS Logs

- When a human is browsing or exploring a Web server, access log entries often show temporal gaps between viewed pages as the individual reads the contents of the pages or assesses the results of the requests.
- A human may misspell a page or return to a particular page several time.

318

Examining IIS Logs

- Web proxies can also be used to conceal the IP address. However, these proxies will have log files showing which computers on the network accessed which Web pages on the Internet.

319

Processing Evidence on MS Exchange

- Microsoft Exchange is tightly integrated with the operating system
  - It is not feasible to restore the Exchange database files and examine them directly.
  - It is necessary to build a restoration server identical to the original server that has the same
    - Computer, site and organization names
    - Versions, service packs, and hot fixes of Windows NT and Exchanges.

320

Processing Evidence on MS Exchange

- The registry in the original server usually contains most of the information that is needed to configure the restoration server.
  - The Microsoft Support Knowledge Base contains articles detailing where some of this information is located.

321

Processing Evidence on MS Exchange

- It may be necessary to install backup software because Exchange runs as a service on the operating system and keeps certain files open at all times.
- To successfully preserve these open files, the backup application must use special processes to save the online email databases files.

322

Information Store Restoration

1. Shut down all of the Exchange services on the restoration server
2. Delete contents in the *Exchsrvr\Mdbdata* folder
3. If the files come from an offline backup, copy the contents of *Exchsrvr\Mdbdata* on the restoration server.

323

Information Store Restoration

4. If restoring from an online backup, restore the Exchange Information Store only.
5. Restart the Exchange System Attendant and Exchange Directory services.

324

Information Store Restoration

6. Open a command prompt windows
   - Change directory to *Exchsrvr\Bin*
     - *cd Exchsrvr\Bin*
   - Run *isinteg* with the *patch* command option
     - *isinteg –patch*

7. Start the remaining Exchange services.

325

Information Store Restoration

8. Open the Exchange Administrator Program
   - Select the restoration server as the server to administer.
   - Highlight *Server Object*
   - View *Properties*
   - Select *Advanced* tab
   - Under *DS/IS Consistency Adjustment*
     - Select *All Inconsistencies*

326

Information Store Restoration

9. The DS/IS Consistency Adjustment will repopulate the Exchange directory.

10. The examiner can now access the mailboxes of specific individuals or accounts.

327

Processing Evidence on MS Outlook

- In many situations, the Outlook email clients will not have sufficient capabilities to perform a full forensic analysis.
- The examiner have to translate email messages and attachment from the .pst file into a format more amenable to searching and analysis.

328

Processing Evidence on MS Outlook

- Email migration tools
  - UniAccess (www.comaxis.com) will extract emails messages out to an HTML format, with hypertext links from messages to their attachments.
  - Exlife (www.ornix .com) will convert the email messages to text files. Attachments are extracted out of the .pst into their native format.

329

Windows Active Directory

- Active Directory (AD) is core components of Win2K
- This central repository for critical data contains
  - User accounts
  - Passwords
  - Email addresses
  - Personal data
  - Security settings
  - Auditing settings

330

Windows Active Directory

- AD is stored on Domain Controllers in
  - *%systemroot%\NTDS\ntds.dit*
  - The *ntds.dit* file can be viewed using the Active Directory snap-in in Microsoft Management Console.

331

This slide is intentionally left blank

332

This slide is intentionally left blank

333

This slide is intentionally left blank

334

This slide is intentionally left blank

335

This slide is intentionally left blank

336

Section 8

Forensics on Unix

337

Forensics on Unix

- Unix recognizes 2 basic user types:
  - Superusers or Root (USERID=0)
  - Ordinary users (USERID!=0)
- When a system administrator creates a new user account, the system acknowledges the new user by adding user entries in the */etc/passwd* file.
- The new user is assigned a unique USERID.

338

User Permissions

- When the user logs into the Unix environment, a shell process is executed on behalf of the user.
- The owner of a process is identified by his USERID.

339

User Permissions

- Other processes run on behalf of the user will have the same permission which is known as the *real user-id (ruid)*.
- A user may execute a file owned by root, where *Set User-ID (SUID*) functionality allows the process to run with root privileges.

340

User Permissions

- For example:
  - The */etc/shadow* file contains encrypted passwords and does not allow ordinary users to modify it for security reasons.
  - However, this file is updated when users change their password.

341

User Permissions

- The *passwd* program used to change passwords has *SUID* permission set so that it runs with root (*user-id 0*) privileges.
- This allows ordinary users to update the otherwise locked */etc/shadow* file.
- Listing the *passwd* executable file will show an 's' over the file owner's executable permission, signifying the SUID permission.

342

Backdoor to Root

- Reviewing and comparing SUID files to a known baseline for those files, may identify a backdoor that gives an ordinary user root privileges.
- The *find* command will produce a comprehensive list of files with the SUID/SGID permission set.
  - Set Group-ID (SGID) permission allows an executing process to inherit the group privileges rather than the file owner privileges.

343

Shared Files

- Special attention should be given to world-writeable files, especially system files.
  - Anyone can place a malicious code on the system.
- To list all world writeable files

```
# find / -type f \( -perm -2 -o -perm -20 \) -exec ls -l {} \;
# find / -type d \( -perm -2 -o -perm -20 \) -exec ls –ld {} \;
```

344

File Hashes

- When analyzing a system without baseline files, examiners must create or obtain their own.
- Creating a baseline may involve installing the operating system or coordinating with vendors for a baseline.
- Sun@Micosystems' Solaris Fingerprint Database contains close to 1 million *md5sum* hash entries of trusted binaries.

345

File Hashes

- After installing the subject operating system
  - Create a *md5sum* hash of the targeted system binary directories
    - /bin
    - /usr/bin
    - /sbin
    - /usr/sbin.
  - Compares the two files using the Unix command *diff*.

346

System Configuration

- The */etc/syslog.conf* file sets the facility and priority level of individual logs.
  - Facility is the service that an event will originate
  - Priority is the extent to which logging will occur.
  - The facility and priority make up one field, separated by a period.

347

Facility Levels

Auth	Security and Authorization-related commands
Authpriv	Private authorization messages
Cron	The cron daemon
Daemon	System daemons (may cause redundant logging)
Kern	The kernel
User	User process
News	Usenet mews system
Mail	Mail system

348

Priority Logging Levels

Emerg	Panic situation
Alert	Urgent situation
Crit	Critical situation
Err	Other error conditions
Warning	Warning messages
Notice	Unusual occurrences
Info	Usual occurrence
Debug	All occurrence

349

System Services

- Some Unix services are specifically initiated or terminated based upon the configuration of scripts located in the */etc/rc* directories.
- The directories are named according to run level and each script starts with
  - S for start, K for kill
  - For example
    - */etc/rc**3**.d/**S**80sendmail* is the sendmail **S**tartup script initiated at run level **3**.

350

System Services

- Examiners can get an idea of what services are launched by understanding the Unix scripting and services.
- Other services are initiated when needed by a daemon that listens for network requests.
  - This daemon is called the Internet Daemon and is controlled by */etc/inetd.conf.*
  - This file will provide the name of the service, the type of delivery, protocol, wait status, uid, server and any arguments.

351

User Accounts

- The */etc/passwd* file identifies
  - User account names
  - User and group ids
  - User general information
  - User home directory
  - User shell
  - If it contains password hashes, the system is vulnerable to password cracking.
    - Password hashes are commonly protected in the */etc/shadow* files.

352

User Accounts

- User-id 0 should be reserved for root only.
- Any other shared user-id 0 should be questioned.
- Verify that daemon accounts, including 'nobody'
  - Do not reference a user shell
  - Should state */bin/false*

353

Scheduled Jobs

- Intruders sometimes create scheduled jobs to ensure that certain malicious processes stay running.
  - On Linux, scheduled jobs are in found */etc/cron.d*
    - These jobs are run at intervals determined by */etc/crontab*.
  - Other Unix systems store cron jobs in */var/spool/cron/crontabs.*
    - The binary file */usr/bin/crontab* runs as the effective user (suid) root.

354

Standard Unix Logs

wtmp /wtmpx	Keeps track of login and logouts. Grows in length and is extended to wtmpx. The *last* command refers to this file for information
utmp /utmpx	Keeps track of users currently logged into the system. Provides output for the commands *w, finger* and *who*.
Lastlog	Keeps track of each users most recent login time and records their initiating IP Address and terminal

355

Standard Unix Logs

Sulog	Records the usage of the *su* switch user command.
Httpd	Tracks originating IP address of WWW connection.
History files	Keeps a record of recent commands used by the user. Usually kept in the users *$HOME* directory.
Router logs	Witness system.

356

Standard Unix Logs

syslogd	A daemon that refers to the *syslog.conf* configuration file for detailed logging. The names of further logs are identified. Logs with unique names and locations may be identified in this file.
Messages .[0-X]	Records major events and is usually rolled over into historical logs with naming conventions: *messages, messages.1, messages.2, messages.3*

357

Standard Unix Logs

FTP Logs.xfr	Maintains extensive logs to track incoming connections and typically shows the originating IP address of the connection.
maillog	This is usually facilitated by *syslogd* in the same format. It provides status of mail handling.
Aculog	Records the use of dial out facilities. Records username, time, date and phone number.

358

Standard Unix Logs

acct/pacct	Used to bill users on their CPU usage. Maintains a list of user's commands and their process time they used.
Packet sniffer logs	Captures network IP packets. The administrator may run a packet sniffer to maintain statistics, troubleshoot problems, or overall manage of the network. It is often used to capture usernames and passwords.

359

Login Process

- Unix tracks current and previous activity using *lastlog, utmp* and *wtmp*.
- Each time a user logs into a Unix system, the login program searches *lastlog* file for the user's UID. If found, the time and location where the user last accessed are written to standard output.

360

Login Process

- New login time and hostname are updated in the *lastlog* file.
- The *utmp* file is opened and a record for the user is inserted.
- The *utmp* file contains a list of current logins.
- The *utmp* file is used by *rwho*, *w* and *who*.

361

Login Process

- When the user logs out, the entry in the *utmp* file is deleted.
- Data in the *utmp* file are appended to the *wtmp* file.
- Another record is added when the user logs out, enabling *last* to provide the session duration.

362

Login Process

- The *wtmp* file maintains a history of login activity on the system.
- The *wtmp* file is used by the program *last* and *ac*.
- The default *wtmp* file will increase without bound. It is normally truncated by the daily scripts run by *cron*, which rename and rotate the *wtmp* files.

363

Shell History Files

- The shell history record commands issued in the shell environment, of which the examiner can track commands the intruders issued to the system.
- The history log is stored per-user basis in a user's home directory.

364

Shell History Files

- When multiple-shells are involved concurrently, cached commands are written into a new file after the history file has been deleted.
- Default locations for history files
  - *.history* for C shell (CSH)
  - *.sh_history* or *.ksh_history* for Korn Shell (KSH)
  - *.history* for Bourne Again Shell (BASH)

365

Restoring Tape Images

- Unix system allows many useful ways of looking at the data from the tape.
- Linux provides many useful utilities, additional file systems and device handlers.

366

Restoring Tape Images

- Determine the name of the tape drive
  - Cycle through a loop
  - Substitute each number from a list
- Drive names in SunOS/Solaris
  /dev/ rmt/{drive#:**0**,**1**,**2**}[density indicator:**l**,**m**,**h**,**u**,**c**][**b**erkley][**n**o rewind]
- Drive names in Linux
  /dev/ [**n**o rewind]**st**{drive#:**0**,**1**,**2**}

Determining the Tape Drive

- For Solaris:

```
For drive 0 1 2 3 4 5 6 7 8 9
>do
>mt –f /dev/rmt/$(drive)n status
>done
```


Determining the Tape Drive

- For Linux:

```
For drive 0 1 2 3 4 5 6 7 8 9
>do
>mt –f /dev/nst$(drive) status
>done
```


Determining the Tape Drive

- Look at what SCSI devices are available
  cat /proc/scsi/scsi
- Check the status to ensure the write-protection has been set.
  mt –f /dev/nst0 status

Ensuring Write Protection

- If write-protected, the status shall have the WR_PROT flag set.
  - 8 mm tapes
    - Protected if red tab is covering the hole
    - Unprotected if hole is visible
  - 4mm DAT tapes
    - Protected if white tab is opened
    - Unprotected if white tab is closed

Determining the Block Size

- Set the block size to zero in order to automatically seek the block size used
  mt –f /dev/nst1 setblk 0
- Common block sizes
  - 521 bytes for *dd*
  - 10240 bytes for *tar* or *cpio* .
  - Some proprietary backup commands use block sizes that adjust or vary throughout the tape.
    - In this instance, use *tcopy* to copy the data

Determining the Block Size

- Read one block with the tape drive on automatic and check how big it is.

#dd if=/dev/nst1 of=test_file count=1 bs=512k

Source Destination Read only 1 Block Block Size

– Rewind the tape to the beginning
– *#mt –f /dev/nst1 rewind*

373

Checking the File Type

- Verify the type of data stored on the tape
  # dd if=/dev/nst2 count=1 |file –
  - The *file* command will give an indication for most formats of *tar, cpio* and *backup*
- The examiner should use the appropriate command to restore the data from the tape.

374

Checking the File Type

- Most tape will have header information on the file type.
- If the *file* command does not give a clear determination of the type of data, examine the file manually using
  – *xxd* (hex dump)
  – *od* (octal dump)

375

Manual Tape Copy

- Duplicate a copy and store the original evidence away.

 # mt –f /dev/nst0 setblk 1024 Set Block Size on Source, with No Rewind
 # mt –f /dev/nst1 setblk 1024 Set Block Size on Destination, with No Rewind
 # dd if=/dev/nst0 of=/dev/nst1 bs=1024

– Repeat the *dd* commands until all files on the tape have been copied.

376

Identifying Attached Hard Drive

- Disk drives are generally of two main types
  – IDE
  – SCSI
- On Linux IDE
  – Primary controller
    - Master drive is */dev/hda*
    - Slave drive is */dev/hdb*
  – Secondary controller
    - Master drive is */dev/hdc*
    - Slave drive is */dev/hdd*

377

Identifying Attached Hard Drive

- Linux partitions
  – Partitions will add a number: *hdb1, hdb2, hdb3* and *hdb4* for the primary partitions.
  – Extended partitions start with *hdb5, hdb6* and so on.
- Sun partitions
  – Disks are numbered from 0 to 7.
  – Slice 2 is referred to as the 'backup slice.

378

Identifying Attached Hard Drive

- SCSI disk devices
  - Typical names are */dev/sda* and */dev/sdb*.
  - The first SCSI disk device detected will be letter *a*, the second *b* and so on.
  - A failure or removal of a driver or SCSI controller card may cause the name of a drive to suddenly change.

379

Identifying Attached Hard Drive

- SCSI disk devices
  - File systems automatically mounted at boot time may no longer function if a failure is encountered.
  - All drivers required for boot should be verified and mounted manually to protect the evidence.
    - Automatic mount at boot only recommended for Linux IDE.
  - SCSI drives have a physical write-protect jumper that can be set to provide write protection.

380

Identifying Attached Hard Drive

- The *fdisk* command for Linux is very useful in listing drive and partition information on block devices.
- Examiners may verify what devices they expected to see through the partition information.

381

Clearing a Hard Drive

- Clear the new disk of all data
  - *sync* ensures all buffer caches are written to disk

```
# dd if=/dev/zero of=/dev/sdb; sync
```

- Verify that the disk has been cleared by dumping the device out to display all non-zero bytes.

```
# dd if=/dev/sdb | xxd | \
grep –v "0000 0000 0000 0000 0000 0000 0000 0000"
```

382

Duplicating a Hard Drive

- Disk duplicate can also be performed using

```
#dd if=/dev/sda of=/dev/sdb; sync
```

- Verification can be performed using *md5sum*

```
# dd if=/dev/sda | md5sum
# dd if=/dev/sdb count={# of records} | md5sum
```

  - If the destination drive is larger than the block count limit, it will have to be added to ensure that the *md5sum* does not consider the trailing zeroed bytes.

383

Mounting a Hard Drive

- Use the *mount* command to
  - Show devices already mounted on the system.
  - Verify what mount points already been used.
  - Make available the logical files within the file systems.

384

Mounting a Hard Drive

- Show that the file system is available logically and is read-only.
- Use the loop option to ignore cylinder /head/sector parameters and access the block device block by block.

#mount –r –t ufs –o loop /dev/sdb1/TARGET

385

Unix System Logs

- The *last* command is used to query *wtmp* log files to determine who logged into a system and when they logged out.
  - The *last* command on most system truncates hostname.

386

Unix System Logs

- Not all programs makes an entry in *wtmp* in all cases.
  - The *sshd* does not make an entry in *wtmp* when using *scp* port forwarding.
- The *wtmp* log can be corrupted by an incomplete write
  - Hence necessary to analyze log entry using customized programs

387

Unix System Logs

- *syslog* sends information to a central logging host using the UDP protocol.
  - UDP is an unreliable connectionless protocol.
  - *syslog* timestamps the log entry with the date and time of the syslog server, not the sending host.
    - This can introduce a time discrepancy.
  - The syslog server has no way of confirming the origin of a given log entry.
    - Hence possible to forge a log entry and send it to the syslog server.

388

Unix System Logs

- For added security, use *tcp_wrappers* to restrict access to a server and generate more detailed entries in the system logs.
- Not all programs can be wrapped using *tcp_wrappers*, hence host-based firewalls are often used to restrict access.

389

Unix System Logs

- Host-based firewalls can create very detailed logs because they function at the datagram level, catching each datagram before it is processed by *tcp_wrappers*.
  - Firewalls can log all connections to a host, both those permitted and rejected.

390

Unix System Logs

- Sun has a Basic Security Module (BSM) that creates audit records similar to NT Event Logs in a binary format.
  - To convert the binary audit logs into readable text, use
    - *praudit*
    - *auditreduce*
    - *BSM Event Viewer*

391

Unix System Logs

- Web Servers
  - Web servers such as Apache and Netscape running on Unix have log files similar to the Microsoft Internet Information Sever.

392

Unix System Logs

- Email Servers
  - Simple Mail Transfer Protocol (SMTP) is used to deliver email over the Internet.
  - Post Office Protocol (POP) enables individuals to read email by downloading it from remote server.
  - The Internet Message Access Protocol (IMAP) enables individuals to view email while residues on the server.

393

Unix System Logs

- SMTP servers do not usually require a password. Thus, it is
  - Easy to forge messages
  - Difficult to prove that a specific individual sent a given message.

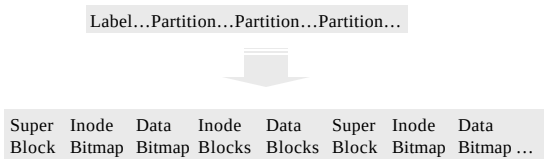
394

Unix System Logs

- POP and IMAPO servers require username and passwords before providing access to the personal email.
- Thus, if a message has been deleted from the server, there may still be evidence of its existence in the server's log files.
  - SMTP servers keep logs that pass through.
  - IMAP and POP servers keep logs of who checked emails.

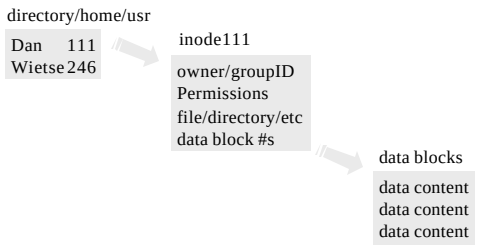
395

Unix File System



396

Disk blocks



397

File Types

- Regular file
- Directory
- Symbolic link (alias for other file)
- Device (e.g., terminal, disk, memory)
- Inter-process communication: named pipe, socket

398

File System Properties

- Everything is placed in one logical tree.
  - No C: or D: drives
  - Even devices are accessible through the file system.
- Directories are files
  - Except that users can't write to them
  - Some remote file systems may disallow reading
- Files may contain holes
  - No data is written in holes
  - Holes read back as all-zero blocks

399

File System Properties

- Multiple references are possible for a file
  - A file can appear in multiple places, even in places owned by different users
- Zero references are also possible
  - A file can still exist after it is removed
- No built-in undelete provision like DOS
- Wasted space only 0.5 kbytes at the end of a file

400

File Attributes

- Ownership
  - Numeric user and group ID
- Permissions
  - Read, write, execute for owner, group, other
- Types
  - File, directory, symlink, device
- Reference count
- File size in bytes
- Time stamps
  - MAC times

401

Physical Locality

- Modern UNIX file systems do not scatter the contents of a file randomly over the disk to avoid fragmentation
- The file system locality allows deleted file contents, access time patterns and other attributes to survive long after a file is deleted
- When a file is deleted, the system makes only minimal changes to the file system

402

Permanency of Delete Content

- A really secure delete takes time
- It is possible to recover data from the disk even after overwriting multiple times
- It is possible to recover data from the RAM after powering off

403

To Wipe a UNIX System

- Wipe files before removing them
- Wipe free space
- When shutting down the system
  - Wipe swap space
  - Wipe memory
- Wiping software
  - http://thc.pimmel.com/

404

Grafting to Hide Effects of Wiping

- All-zero free blocks are unusual
  - Raise suspicion of wiping
- Solution
  - Overwrite free space with plausible data
- Cloning/grafting
  - Use copies of recently accessed files from the system
    - Eg. mail, program source code, web pages/images

405

Effects of File Deletion: Directory

- The directory entry with the file name is marked as unused
- The file name becomes disconnected from any file information
- Names of the deleted file can still be found by examining a directory with the *strings* command
- Linux does not allow directories to be accessed in this manner.
  - Use the *icat* utility to work around this restriction

406

Effects of File Deletion: Inode

- The inode file attribute block is marked as unused in the inode block allocation bitmap
- Some file attribute information is destroyed, but a lot of information is preserved
- Linux preserves the connections between the file inode block and the first 12 file data blocks

407

Inode Information for Deleted File

- Ownership:
  - Numeric user and group ID
- Permissions:
  - Read, write, execute for owner, group, other
- Types:
  - File, directory, symlink, device, FIFO, socket
- Time stamps:
  - Last file Modification
  - Last file Access
  - Last status Change
    - Owner, permissions, refcount
- Reference count
  - Zeroed when removed
- File size in bytes
  - Zeroed, except LINUX
- List of data block numbers
  - Zeroed, except LINUX

408

Effects of File Deletion: Data Blocks

- File data blocks are marked as unused in their block allocation bitmap
- Contents in the file data blocks are left untouched
- File data blocks are no longer connected with the file
- Linux has an option to erase file data blocks upon file deletion, also the first 12 data blocks remain connected to the inode block

409

Effects of File Deletion: Summary

•Directory	
–Name	Preserved, disconnected from file
•Inode attributes	
–Owner	Preserved
–Group ownership	Preserved
–Last read access time	Preserved
–Last write access time	Preserved
–Last attribute change time	Time of Deletion
–Delete time (in Linux)	Time of Deletion
–Directory to ref count	Destroyed (Preserved in Linux)
–File type	Destroyed (Preserved in Linux)
–Access permissions	Destroyed (Preserved in Linux)
–File size	Destroyed (Preserved in Linux)
–Data block addresses	Destroyed (Preserved in Linux)
•Data blocks	
–Data contents	Disconnected (Preserved in Linux)

410

Erasing the Tracks

- An intruder may remove exploit source and executable code after they have served their purpose
- As the result of such cleanup activity, the only visible evidence is the last modification time of the directory

411

Finding the Tracks

- When a program is compiled, executed or deleted
  - The compiler processes the source code
    - It creates several temporary files before the executable program pops out.
- When the intruder compiles, runs or deletes an exploit program
  - We can find traces of the deleted files
    - Program source file
    - Executable file
    - Compiler temporary files

412

Finding the Tracks

- Use the *ils* utility to retrieve the file attributes
  - The deleted files have no names, disk names and file inode numbers are used
- Compiler temporary files live in the same file system zone as the */tmp* directory
  - The deleted temporary files is overwritten only when a process needs to create a new temporary file.

413

Access Time Patterns

File Size	MAC	Permissions	Directory	File <Dir-Inode #>
85	**m**..	-rw-r--r--	wietse	<hda6-311549>
10897	mac	-rw-r--r--	wietse	<hda1-2022>
301	mac	-rw-r--r--	wietse	<hda1-2023>
872	mac	-rw-r--r--	wietse	<hda1-2024>
85	.**a**.	-rw-r--r--	wietse	<hda6-311549>
4173	**m**..	-rwxr-xr-x	wietse	<hda6-311550>
4173	.**a**.	-rwxr-xr-x	wietse	<hda6-311550>
1024	m..	drwxr-xr-x	wietse	/home/wietse
85	..**c**	-rw-r--r--	wietse	<hda6-311549>
4173	..**c**	-rwxr-xr-x	wietse	<hda6-311550>

Create source file
#85 <hda6-311549>

Compiler temp file
M = Write/Create
A = Read/Run
C = Change Attribute/Delete

Read source file
Create executable
#4173 <hda6-311550>

Run executable

Delete source file
Delete executable

414

Section 9

Forensics on the Networks

415

Forensics on the Network

- Log files contains large amounts of trace information.
- IP address may not pinpoint the culprit, but it does narrow down the search to a particular machine.
- Server logs record which IP address had used a specific services at a specific time.

416

Forensics on the Network

- IP address are stored in the Web server access log.
- Dialup modem banks and BOOTP/DHCP servers create log files of IP address assignments.
- Firewalls and routers keep log of the TCP/IP traffic passing through (usually incoming).

417

Challenges of Network Analysis

- Evidence is often distributed on many computers.
  - The distributed nature of the networks may make it impossible for investigators to gain physical access to the device that contains valuable evidence.
  - It may be necessary to collect evidence from a remote system or access an active network device to collect volatile data.

418

Challenges of Network Analysis

- Evidence is often present on a network for only a short time.
  - Such information is stored in volatile memory of network devices or in network cables.
  - Windows of opportunity for collecting this volatile evidence is very small.

419

Challenges of Network Analysis

- When collecting network log files, it may not be feasible to shut down the systems
  - Evidence in volatile memory can be lost if the network cable is disconnected or the computer is turned off.
  - It may be difficult to make a bitstream copy of the hard disk.

420

Challenges of Network Analysis

- One approach to gathering evidence from a system entails using the *who* and *netstat* commands to send the results into a file on an external device.
- This technique minimizes the impact on the system when valuable evidence may be stored in slack and unallocated space.

- Encryption is becoming more common, which allows criminals to scramble incriminating evidence.

421

Difficulties of Collecting Network Evidence

- Log files contain overwhelming information at the transport and network layer
- State tables contains activities of many users but are only available for a short time
- Cutting and pasting on segments of a log file is not satisfactory from the evidentiary viewpoint for authenticity and integrity of the digital evidence

422

Network Evidence Collection

- Consider taking print screen snapshots
- Use message digests to preserve the integrity of the original copies of all log files, and perform investigations on duplicate copies
- Cross comparison of the log files can provide a rich source of evidence

423

Collecting Evidence on Network

1. Maintain a log using Unix *script* command or Telnet/SSH session logged to a file. Videotaping.
2. Resolve all IP addresses to obtain their associated canonical names so that both the IP addresses and names are available at a later dates even if the name is changed in the domain name system.

424

Collecting Evidence on Network

3. Use SNMP to obtain information from routers and firewalls.
4. Take *printscreen* with date and time from a trusted time source.
5. Use *traceroute* to document the location of the host being accessed.

425

Collecting Evidence on Network

6. Encrypt and digitally sign all evidence files to preserve the integrity.
7. Seek and collect corroborating information from multiple independent sources.
8. Access log entries in the IDS.
9. Query the DHCP server.

426

Log Analysis

- Look for traffic anomalies
- Look for traffic originating from or terminating on the compromised machines
- Look for broken or unusual patterns in the traffic

427

Network Traffic Reconstruction

- It is not feasible for an examiner to comprehend all traffic by viewing its hex representations.
- Examination tools are required to reconstruct the packets and display them in a way that facilitates analysis.

428

Network Traffic Reconstruction

- *mailsnarf* and *webspy* can reassemble and display application layer data in real time, providing an effective way to monitor an individual's online activities.
- *NetWitness* (www.forensicexplorers.com) has the capability to capture traffic (or read a *tcpdump* file), reconstruct session, display content in real time and analyze the traffic.

429

Network Traffic Reconstruction

- *review* (security@net.ohio -state.edu) can process the original binary data in a *tcpdump* log. By piecing together TCP packets and extracting the original payload, it is possible to obtain files that the intruder downloaded from or uploaded to a system.

430

Routers

- Routers can be configured to keep traffic-related logs.
  - However, routers are often configured with minimal logging to conserve storage space on the central server.

431

NetFlow

- A growing number of routers have *NetFlow* to improve routing performance.
- When the *NetFlow* feature is enabled, routers record detailed information about each flow
  - Current time according to the router
  - Start and end times of the flow
  - Source and destination IP addresses and ports, IP protocol type, number of packets and bytes in the flow.

432

NetFlow

- If the system is compromised, *NetFlow* logs will show
  - The source of the attack
  - Protocols used
  - Ports accessed
  - Amount of data transferred

433

NetFlow

- Once the source of the attack is known, *NetFlow* logs can be searched for other machines on the network that were targeted by the attacker.
- *NetFlow* packets are exported when a flow ends, resulting in a log files with entries sorted by flow end times.
  - Sort *NetFlow* logs using the start time of each flow before attempting to interpret them.

434

NetFlow

- *NetFlow* record does not indicate which host initiated the connection, it only indicates that one host sent data to another host.
  - Therefore, it is necessary to infer which host initiated the connection.
  - Sorting the relevant flows using their start times to determine which flow was initiated first.

435

NetFlow

- *NetFlow* records exported from a router are encapsulated in a UDP datagrams
  - Some of the records may not reach the intended logging server. Thus, the logs may not be complete.
  - Newer *NetFlow* records contain a sequence number that can be used to determine if any records are missing or if forged records have been inserted.

436

NetFlow

- *NetFlo*w records are sometimes exported before a flow is terminated.
  - Thus, a single flow may cause several flow record to be created.
  - In this case, several flow records may have to be combined to determine the amount of data transferred or duration of the flow.

437

Dialup Server

- When an individual dials into the Internet, there are two forms of evidence at the ISP
  - The contents of the terminal server's memory
  - The logs from the associated authentication server.

438

Dialup Server

- The TACACS authentication system keeps records of the time, user name, terminal server and port, and IP address for each login and logout event.
- TACACS assigns code requests dealing with SLIP connections
  - LOGIN (Type=1)
  - LOGOFF (Type=7)
  - SLIPON (Type=9)
  - SLIPOFF (Type=10)

439

Dialup Server

- Restrict the modem pool to authorized users by requiring users to authenticate with a user name and password when they connect.
- The TACACS logs can then identify the account that was used to authenticate access to the modem pool.

440

Dialup Server

- The logs from RAM can be collected using the *show logging* command.
- Each log entry contains the
  - Date and time
  - Facility code
    - SEC, SYS, SSH, BGP
  - Severity
  - Message

441

Dialup Server

- The *show history* command can be used to list the commands executed during the examination.

442

Pen Registers

- A pen registry is a device that is physically attached to a target phone line.
- It records all of the numbers that are dialed through that line with the time and duration of the calls.
- It provides a complete record of incoming and outgoing phone calls for the suspect.

443

Phone Tracing

- Requesting a phone company to trace an intruder presents a problem when dealing with a modem pool
  - Many phone circuits are associated with a single dial-up number
  - Need to correlate the phone traces against the modem pool authentication logs and match phone calls against login sessions.
  - Event lag and clock offset complicates correlating the authentication logs against the phone traces.

444

Phone Tracing

- Phone switch records
  - Server = Terminal server name
  - Line = Port on the terminal server
  - Slip = DNS name for the IP address associated with that port.
- This information can help trace an IP address to a specific terminal server/port and to a unique circuit id, span, channel and trunk for the phone company to trace the circuit in real time.

445

Network Traffic

- To monitor network traffic, sniffers decode datagrams and display them in an easy-to-read format.
- Etherpeek (www.etherpeek.com) provides several views of captured traffic
  - It shows the raw data, the decoded data, and interpreted view showing what the data represent.
  - Etherpeek can also be configured to generate an alert when traffic matching specific criteria is detected.

446

Network Traffic

- When a hub is used, communication between machines on the same network is visible to all machines connected to the hub, making eavesdropping very simple.
- When a switch is used, communication between machines is not visible to all computers on the subnet. However,
  - ARP proxying can be misused to intercept traffic
  - dsniff (naughty-monkey.org/~dugsong/dsniff)

447

Network Sniffer

- *Snoop* is network sniffer installed by default with SunOS/Solaris.
- Entries in the *snoop* are not time-stamped.
  - The *-t* option is required to timestamp entries
  - Timestamps are accurate to within 4 microseconds.

448

Network Sniffer

- Timestamp options
  - *d* Delta Time since receiving the previous datagram
  - *a* Absolute Clock time
  - *r* Relative Time relative to the first datagram displayed
- The absolute time is usually desirable because it can be easily compared with timestamped information from other sources.
- The -p option can be used to display time relative to any selected datagram.

449

Capturing TCP Packets

- *tcpdump* (www.tcpdump.org) can be installed on most versions of Unix and has been ported to Windows.
- *tcpdump* can also be used to capture UDP datagrams .

450

Capturing TCP Packets

- *tcpdump* only captures the first 68 bytes of a datagram by default
  - To collect more information, set a larger snaplen value using the *–s* option.
  - Using a larger snaplen increase the chance of overloading and losing datagrams
- Filters can be used to reduce the amount of information that *tcpdump* collects.

451

Capturing TCP Packets

- *tcpdump* represents TCP flags as follows:
  - S SYN Synchronize sequence numbers, establish connection
  - F FIN Terminate connection
  - R RST Reset connection
  - P PSH Push data, do not buffer before send
  - . No flag set

452

Examining TCP Logs

1. *tcpdump* can contain the complete contents of all network traffic for each of the sessions, including the data portion of the packets.
2. Use the filtering expressions in the *tcpdump* to pull out packets of interest from the total log based on the examination of the packet headers.

453

Examining TCP Logs

3. Use *review* (security@net.ohio-state.edu) as a graphical user interface to browse the *tcpdump* log
4. Look at the summary of the contents of a single log, view the contents of sessions within a log and replay the contents of selected sessions to see an 'intruder's eye view' of the log contents.

454

Merging Logs

- There are some hosts where network traffic goes out through a router and returns through the second (due to asymmetric routing).
- This can also be an issue where there are multiple SMTP servers and for Web proxy servers.
- Sometimes, it is necessary to merge several logs together to reconstruct a complete record of thenetwork activity.

455

X Windows

- Event structures
  - Keystroke
  - Mouse movements
  - Mouse button clicks
- Request structures
  - –Draw lines
  - –Clear regions
  - –Change fonts
- Result structures
  - Response to the requests

456

X Windows

- *xterm* sessions in *tcpdump* logs are recorded in non-human readable binary structures
- A special graphical user interface, e.g. *review*, is necessary to pull out the keystrokes in the *xterm* sessions=

457

Accessing Unix Log Files

- Most log files in
  - */usr/adm*
  - */var/adm*
  - */var/log*
  - */etc*
- To view log files
  - *vi*
  - *more* (syslog)
  - *who* (utmp)
  - *last* (wtmp)

458

Accessing Unix Log Files

- *acct* or *pacct*
  - Accounting logs contain commands typed by every user
- *Aculog*
  - Contains a record of when modems were used to dial out
- *lastlog*
  - Contains a record of each user's most recent login or failed login

459

Accessing Unix Log Files

- *loginlog*
  - Records failed logins
- *sulog*
  - Records every attempt to log in as the administrator of the computer (root).

460

Accessing Unix Log Files

- *messages* or *syslog*
  - Main system log file containing wide range of messages from various applications. Routers and firewalls can be configured to add their messages to this file.
- *utmp* and *utmpx*
  - Contains records of all users currently logged into a computer.
  - File saved in */etc*

461

Accessing Unix Log Files

- *wtmp and wtmpx*
  - Contains a record of errors that are encountered when accessing external media
  - File saved in */etc*
- *xferlog*
  - Contains records of all files transferred from a computer using the FTP

462

syslog

Jan 1 23:45 mycomputer sendmail[11668]: "debug" command from **hacker.dhp.com (199.245.105.25)** *Attacker IP address*

Jan 1 23:45 mycomputer sendmail[11668]: "wiz" command from hacker.dhp.com (199.245.105.25)

Jan 1 23:46 mycomputer sendmail[17936]: TAA17936: ruleset=check_rcpt, arg=someone@hotmail.com, relay=**08-162.015.popsite.net** [**207.240.169.162**], reject=550 *Dial in connection* *Source of junk mail*

<21freeto@flashmail.com>…Relaying denied

Jan 1 23:47 mycomputer sendmail[17936]: TAA17936: from=smoke@www.lg.co.kr,

size=0, class=0, pri=0, nrcpts=0, proto=SMTP, relay=08-162.015.popsite.net [207.240.169.162], reject=550 someone@hotmail.com….Relaying denied

syslog

Jan 1 23:48 mycomputer **rshd**[7373]: connection from 199.245.105.25 on**illegal port 2066**
Jan 1 23:48 mycomputer **ftpd**[7375]: connection from hacker.dhp.com
Jan 1 23:49 mycomputer login[7593]: failed ?@ hacker.dhp.com as **+**
Jan 1 23:49 mycomputer login[7595]: failed ?@ hacker.dhp.com as **bin**
Jan 1 23:50 mycomputer login[7596]: failed ?@ hacker.dhp.com as **daemon**
Jan 1 23:50 mycomputer login[7597]: failed ?@ hacker.dhp.com as **lp**
Jan 1 23:51 mycomputer login[7599]: failed ?@ hacker.dhp.com as **nuucp**
Jan 1 23:51 mycomputer login[7600]: failed ?@ hacker.dhp.com as **root**
Jan 1 23:52 mycomputer login[7604]: failed ?@ hacker.dhp.com as **user**
Jan 1 23:52 mycomputer login[7605]: failed ?@ hacker.dhp.com as **uucp**
Jan 1 23:53 mycomputer **ftpd**[7654]: connection from hacker.dhp.com
Jan 1 23:53 mycomputer **telnetd**[7653]: connection from hacker.dhp.com
Jan 1 23:54 mycomputer **rshd**[7652]: connection from 199.245.105.25 on**illegal port 4128**

Trial and error login attempts

Remote login attempts

Cautions When Accessing Unix Logs

- On some UNIX systems, *wtmp* and *utmp* files truncate the source host name for remote login sessions to some limited size.
  - This obscures the source host name if it is long.
- One approach to addressing this problem is to modify the *last* command to display full hostnames.

Cautions When Accessing Unix Logs

- Accounting records only contain the name of the binary that was executed and not the full path name to the file.
- Need to search all attached file systems for executable files with the same name.

Cautions When Accessing Unix Logs

- In shell scripts, the name of the interpreter for the script is recorded, but the name of the script is not recorded.
- The name of the executable can be inferred based on the shell history files and by examining the user's *PATH* environment variable settings.

Cautions When Accessing Unix Logs

- Shell history files are typically owned by the account whose activity they record, and so are subject to editing and erasure.
- Shell history is also written when each shell exits, so overlapping shells can obfuscate the record.

Cautions When Accessing Unix Logs

- The *syslog* timestamp that appears on the entries in the log files is the time that the entry was received by the local machine according to its own clock, not the clock of the machine that the log entries come from.
- This can cause confusion if the examiner tries to correlate those log entries to other events from the original host, since there may be a clock offset between that host and the *syslog* host.

469

Accessing WinNT Log Files

- Log files in
  - *%systemroot%\system32\config*
  - *C:\winnt\system32\log*
- *appevent.evt* - log of application usage
- *secevent.evt* - log of security related activities
- *sysevent.evt* - log of system events

470

WinNT State Tables

Log of current and recent connections only!

Date	Time	Source	Category	Event	User	Computer
1/23/00	10:10:02 AM	Security	System Event	515	SYSTEM	ORGO
1/23/00	10:09:02 AM	Security	Privilege use	577	SYSTEM	ORGO
1/23/00	10:07:02 AM	Security	Logon/Logoff	528	ANONYMOUS	ORGO
1/23/00	10:07:02 AM	Security	Logon/Logoff	528	ANONYMOUS	ORGO
1/23/00	10:05:04 AM	Security	Privilege use	578	eco3	ORGO
1/23/00	10:05:02 AM	Security	Logon/Logoff	538	eco3	ORGO
1/23/00	10:04:33 AM	Security	Privilege use	576	eco3	ORGO
1/23/00	10:03:02 AM	Security	System Event	529	SYSTEM	ORGO

Security Log

1/23/00	10:10:10 AM	NETLOGIN	None	5719	NA	ORGO
1/23/00	10:09:11 AM	EventLog	None	6006	NA	ORGO
1/23/00	10:08:12 AM	Dhcp	None	1005	NA	ORGO
1/23/00	10:06:13 AM	Serial	None	6007	NA	ORGO

System Log

471

Log of TCP/IP Connections

netstat –f inet lists all TCP/IP connections

Dial up connections

TCP Local Address	Remote Address	State
www.forensic-science.com.telnet	23.oakland-01.ca.world.net.2048	Established
www.forensic-science.com.telnet	sdn-ar-004njnbruP047.dialnet.1754	Established
www.forensic-science.com.80	dial55175.mru.ru.1084	Established
www.forensic-science.com.80	proxy-354.public.net.43883	Time_Wait
www.forensic-science.com.80	line1.old.net.4667	Fin_Wait_2

Web connections

472

Forensics in the Datalink Layer

- The datalink and physical layers are the richest sources of digital evidence
- Data captured using a sniffer can be very useful in
  - Reconstructing a crime
  - The accuracy of the entries in the logs is based on the confirmation that they have not been manipulated

473

Forensics in the Datalink Layer

- Datalink layer addresses (MAC addresses) are more identifying than the Network layer addresses (IP addresses)
  - A MAC address is directly associated with the Network Interface Card in a computer
  - An IP address can be easily reassigned to different computers

474

ARP Cache

- The Address Resolution Protocol is used by routers to map an IP address to the MAC address of a particular computer
- The ARP cache on a computer or router can be retrieved using *arp –a*

475

ARP Cache

- The ARP cache does not keep permanent record and must be examined shortly after the connection has occurred
- Some routers can be configured to detect incorrect IP addresses to identify computers that have been purposefully reconfigured to hide the user's identity

476

Intrusion Detection System

- *Snort* (www.snort.org) inspects traffic and only stores data that are suspicious.
- The IDS keeps a log of attacks at the network level, allowing the examiner to determine the attacker's IP address.

477

Intrusion Detection System

- Unlike *tcpdump*, *Snort* can
  - Inspect the datagram payload
  - Decode the application layer of a datagram
  - Compare the datagram contents with a list of rules.
  - Configure rules to detect specific types of datagrams
  - Reassemble fragmented packets before checking them against known attack signature
  - Capture the entire binary datagram and store it in a *tcpdump* format.

478

Reliability of Logs

- Logs vary in the degree to which they can be relied upon to be accurate.
  - *utmp* and *wtmp* logs on some UNIX systems are world writable
  - Any user can modify their contents.

479

Reliability of Logs

- The reliability of the logs is dependent on the integrity of the systems that generate the logs.
  - If those subsystems have been compromised or replaced, the logs that they generate may not be a complete or accurate portrayal.

480

Reliability of Logs

- The accuracy of the logs is also subject to the security of the network protocols used for transporting the messages.
  - *syslog* and *NetFlow* logs are both sent using UDP.
  - The logs can be incomplete.
  - It is relatively easy to create false entries by directing carefully crafted UDP packets with spoofed source addresses to the log servers.

481

Reliability of Logs

- Guard against the dangers of incomplete or incorrect logs by correlating events from as many sources as possible and account for discrepancies between the logs.

482

Time-Related Issues

- Most log files include some sort of time stamp which can be used to correlate entries from several logs against one another.
- One common problem is that the clocks on those hosts may not be synchronized.
- It is also important to know the time zone that each log was recorded in. Unfortunately, the timestamps in many logs do not include the time zone.

483

Time-Related Issues

- Event lag is the difference in times between related events in different types of logs.
  - There can be significant event lag between the start of a phone connection and the start of an authenticated session on the modem pool.

484

Time-Related Issues

- Since the amount of lag is often variable, events should not be correlated specifically by starting time or even duration, since the session in the network traffic log would last longer than the login session.
- However, most of the log entries associated with a login session on a host should fall within the start and end times of that session.

485

Time-Related Issues

- Sometimes logs are created in order of the ending time of a session, instead of the start time and this can lend further confusion to the correlation process.
  - Log entries for *NetFlow* logs are created when the flow of traffic ends.
  - UNIX process accounting logs are created when the associated process ends.

486

Time-Related Issues

- Since the ending events often match up more closely in time, it is advisable to use the end time of a session for making correlations
- It is also trivial to leave a process running in the background so that it will persist after logout (using *nohup*), in which case its process accounting records will not be bounded by the login session.

487

DNS Problems

- Intruders can steal domains, poison the caches on DNS servers, or inject false information into address/name lookups.
- Many subsystems resolve the IP addresses that they know into names using DNS and then only log the resolved names which may not be correct.
- Thus, it is necessary to log messages with both the IP addresses and the resolved names.

488

Forensics on the Internet

- Investigating criminal activity of the Application layer
  - Web Browser
  - Email
  - Usenet
  - IRC

489

Forged Emails

Email clients can be configured with false information when communicating with the MTA.

The trusted Mail Transfer Agent is then exploited to relay the forged mails.

490

Email Forgery

```
> HELO Fake.message.com
> MAIL FROM: fake@spoofedaddress.com
> RCPT TO: you@emailaddress.com
> DATA
Subject: Spoofed Email
Date: date and time stamp 1
        This is a forged message.
> QUIT
```

Forging an email on SMTP (Simple Mail Transport Protocol)

```
Date: date and time stamp 1
From: fake@spoofedaddress.com
To: you@emailaddress.com
Subject: Spoofed Email

        This is a forged message.
```

Message at Recipient

491

Email Tracing

Received header of Email show Mail Transfer Agents along the route taken by the message

MTA 2
MTA 1

```
Received: from trustedmta.com by yourmailserver.emailaddress.com
(5.61/1.34) Id AA1404; date and time stamp 2
Received: from fake.message.com (corpus.delicti.com [207.244.93.93])
by trustedmta.com (8.8.5/8.8.5) with SMTP id VAA01050 for
<you@emailaddress.com; date and time stamp 1
Date: date and time stamp 1
Message-Id: <19970707070121.VAA01050@trustedmta.com
From: fake@spoofedaddress.com
To: you@emailaddress.com
Subject: Spoofed Email
```

Real Sender

492

Tracing the Sender

Don't be fooled by a fake sender email account

Information from Received Header
Domain Name
IP Address

Useful Tools
finger
ph
telnet
who is

Find Real Sender
Location
Identity
Intentions

493

Usenet Forgery

> GROUP: alt.abuse
> POST
Subject: Spoofed Article
Path: abc!net
From: nobody@hotmail.com
Newsgroups: alt.abuse
This is a forged message.
> QUIT

Forging an article on NNTP (Network News Transport Protocol)

Path:news. corpusdelicit.com!plne!extra.newsguy .com!lotsanews.com!news. maxwell.syr.edu!news feed.wli.net!su-newshub1.bbplanet.com!Newsbbn. planet.com!newsfeed.concentric.net!master0.new s.internet.net!abc!net
From: nobody (nobody@hotmail.com)
Newsgroups: alt.abuse
Subject: Spoofed Article
Date: date and time
Message-ID: 8pF762$Flg@masters0.internet.net
NNTP-Posting-Host: **cheat.usenet.com**

This is a forged message.

Message at Posting Host

494

Usenet Tracing

News server path

Path: news. corpusdelicit.com!plne!extra. newsguy.com! lotsanews.com!news. maxwell.syr.edu! newsfeed.wli.net! su-newshub1.bbplanet.com!newsbbnplanet.com!newsfeed. concentric.net! **master0.news.internet.net!abc!net**
From: nobody (nobody@hotmail.com) *Check log of this node*
Newsgroup: alt.abuse
Subject: Spoofed Article
Date: date and time
Organization: Nobody's Home
Message-ID: 8pF762$Flg@masters0.internet.net
Reply-To: nobody@hotmail.com *Forged sender information*
NNTP-Posting-Host: **cheat.usenet.com**
X-Trace: SOLAIR2. masters0.internet.net **922191688 24958.199.166**

Dial up connection

495

IRC Tracing

2 main problems

- Communications are transient and hence not archived
- Communications can also bypass IRC network once Direct Chat Mode (DCC) or file server (fserver) is established.
  - IRC clients send information directly to IP address of opposite party

496

IRC Tracing

- */whois* nickname
  - Uses a person's IRC nickname to get the person's email address, chat channel, IRC server chatting on, IP address.
- */whowas* oldnickname
  - To obtain logged information from the IRC server's temporary cache if the culprit leaves the IRC or changes his nickname
- */who* *domain-name* or *pen-name*
  - Searches subnet for any information associated with the culprit

497

Identifying the Intruder

1. Log all packets related to a particular logon session.
2. Invoke *tcpdump* on the targeted host on login and terminate on logout and log all actions to a history file.
3. Track the channel the intruder typically hungs out on to the account used for authentication, and map to the compromised account and IRC nicknames.

498

Identifying the Intruder

4. Monitor suspicious activities such as
   - Several different people connecting to IRC through the compromised account
   - Multiple simultaneous logins
   - Use of accounts for people who were no longer affiliated
   - Intrusion and denial of service attacks

499

Digital Evidence on the Internet

- Digital evidence is often stored on remote servers
- The evidence can be stored in many different places to complicate search
- Creating a cohesive reconstruction can involve a large amount of evidence from a wide variety of sources:
  - Phone traces, pen registers, *NetFlow, tcpdump* logs, authentication logs, victim host logs and host based evidence

500

Digital Evidence on the Internet

- Seizing evidence directly from the remote servers is sometimes impossible
- Ensure that evidence collected from the Internet is authentic and not modified during transmission

501

Digital Evidence on the Internet

- Web browser, email clients, newsgroup activity and log files on the local computer also keeps records of the pages visited, copies of emails and live chats
- Do not change file names for documentary purposes or edit contents of files to make them more readable

502

This slide is intentionally left blank

503

This slide is intentionally left blank

504

Section 10

Forensics on an Unknown Program

505

Identifying an Unknown Program

- Run the program, see what happens.
  - What if the program turns out to be destructive?
- Run the program on a sacrificial machine.
  - What if the program depends on specific machine features?
- Static analysis of program file
  - Slow, but hopefully safe.
- Details will be somewhat operating system specific

506

Analysis Tools

- Program file analysis tools
  - *strings* shows clear-text strings embedded in any file
  - *grep* searches for specific strings
  - *file* identifies file content by looking at part of the data
- General file analysis tools
  - *nm* displays compiler and runtime linker symbol table
  - *ldd* identifies dynamic libraries used
  - disassemblers, debuggers

507

Identifying an Unknown Program

```
% ls -l a
-rwxr-xr-x 1 wietse staff 67724 Jul 24 18:21 a
% file a
a: ELF 32-bit MSB executable SPARC Version 1, dynamically linked, not stripped
```

An executable program

Not stripped, so a lot of compiler information is still available

508

Clues from Symbol tables

Compiler symbol table reveals internal procedure names

```
% nm -p a
0000077448 T nfsproc_getattr_2
0000078888 T nfsproc_create_2
0000079428 T nfsproc_link_2
0000077988 T nfsproc_lookup_2
```

Run-time linker symbol table reveals calls of external shared library routines

```
% nm -Du a
perror
pmap_getport
pmap_rmtcall
printf
qsort
```

509

Finding Exploit Code

- A combination of:
  - MAC time
  - *unrm*
  - *grep* program files for source code
- Standard Unix tools
- Reconstructing mail files
- Text-based log files
- Correlator (binary, repeating logs, etc.)
- File sanity checking

510

Embedded Strings

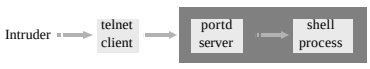
```
% strings - a
- umount remote file system export
- show all exported file systems umountall
- umount all remote file systems umount
[-upTU] [-P port] <path> - mount file system
mount
<local-file> [<remote-file>] - put file
<uid>[.<gid >] <file> - change owner
chown
<mode> <file> - change mode
chmod
<dir> - remove remote directory
rmdir
<dir> - make remote directory
mkdir
<file1> <file2> - move file
<file1> <file2> - link file
<file> - delete remote file
```

511

Backdoor Service

- Stand-alone telnet server
- Bypass TCP wrapper and system login procedure

```
% telnet victim 5120
Trying 131.155.210.17...
Connected to victim.
Escape character is '^]'.
password
SunOS UNIX (victim)
victim#
```



512

Eradicating Network Traces

- It is virtually impossible in most cases for the intruder to eradicate network traces
  - Don't know where data was saved
  - Must determine where data flow went
  - Compromise all routers, hosts, etc.
  - Destroy all information there, plus recursively follow this list

513

Network Sniffing & Spying

- IDS often ineffective by themselves
- Useful for damage control, not for data recovery
- Best as standalone monitoring system
- Requires lots of storage for complete traffic
- Must protect the system(s) doing the sniffing and storing data
- Encrypted or hidden connections a problem

514

Gathering Information

- System configuration
- System and user programs
- System and kernel memory
- Raw memory & disk
- Anything with IP #/hostnames

515

System Configuration

- Enter into the realm of auditing
- Invisible changes
- Freezing system should gather most of this
- Need to know how system should look like
- Kernel
- Packet filters

516

System Configuration

- Access control
  - hosts.allow, httpd.conf, sshd_config
- Trust
  - servers, rhosts, network information
- Configurations
  - routes, inetd.conf, startup files
- Protocols
- User
  - .rhosts, .forward)

517

Programs

- Queries to system
  - *netstat*
  - *arp*
  - *lsof*
  - portscanners
- Program memory
- Logs
  - Syslog
  - NFS
  - NIS
  - DNS
  - Kernel

518

Show Net Status

Active Internet connections (including servers)

```
% netstat -a -f inet
Protocol    R-Q  S-Q  Local Address        Foreign Address      State
tcp    0    0    flying.smtp          192.215.43.108.4778  EST
tcp    0    0    flying.http          dialup6929.nssl..2787  EST
tcp    0    0    flying.smtp          192.215.43.108.4769  WAIT
tcp    0    0    flying.http          telapex..2198        SYN_RCVD

% netstat -rn
Destination  Gateway          Flags  Refcnt  Use      Interface
127.0.0.1      127.0.0.1        UH     1       1365     lo0
default      209.179.181.129  UG     17      2089112  le0
```

Routing tables

519

Portscanners

- *% tcp_scan <udp> 1-1024*
  - 21: ftp
  - 23: telnet
  - 25: smtp
  - 53: domain
  - 515: printer
  - 667: unknown

520

Data Binding

- Keeps track of every query of host
- Send a passive signal to bind
- Dumps database into named_dump.db
- Compare system logs, known hosts
  - use TTL vs time left in memory

521

TCP Wrapper Alert

- Suspicious activity at some unlikely hour

```
Feb 13 23:09:52 wsbs06 in.fingerd[15900]: connect from lock@wsbs03
```

- Screen saver accounts don't finger around at midnight.
- Suspect screen saver account compromised

522

Compromised Root Account

```
Feb 13 23:05:34 wsbs01 in.fingerd[7948]: connect from root@wsbs03
Feb 13 23:05:35 wsbs06 in.fingerd[15895]: connect from nobody@wsbs01
Feb 13 23:05:36 wsbs06 in.fingerd[15897]: refused connect from nobody@localhost
```

 # finger @localhost@wsbs06@wsbs01

wsbs06 ⟵ wsbs01 ⟵ wsbs03

Suspicious Process

 # ps aux

USER	PID	%CPU	%MEM	SZ	RSS	TT	STAT	START	TIME	COMMAND
root	0	0.0	0.0	0	0	?	D	Jan 14	0:01	swapper
root	1	0.0	0.0	52	0	?	IW	Jan 14	0:00	/sbin /init -
root	2	0.0	0.0	0	0	?	D	Jan 14	0:00	pagedaemon
root	75	0.0	0.0	16	0	?	I	Jan 14	0:00	(biod)
root	55	0.0	0.0	68	0	?	IW	Jan 14	0:00	portmap
root	**12823**	**0.0**	**0.0**	**48**	**0**	**?**	**IW**	**23:02**	**0:00**	**<defunct>**

Process name: misleading to hide real purpose.
Process start time: matches time of incident.
Process privileges: super-user

ps incantations (BSD)

Basic listing

 # ps ax

PID	TT	STAT	TIME	COMMAND
152	p0	S	0:00	-csh (csh)
883	p0	R	0:00	ps ax

Command and environment listing

 # ps auxeww

USER	PID	%CPU	%MEM	SZ	RSS	TT	STAT	START	TIME	COMMAND
Wietse	152	0.0	1.5	56	212	p0	S	09:12	0:00	-csh

HOME=/home/wietse USER=wietse LOGNAME=wietse PATH=/bin:/usr/bin:
/usr/ucb :/usr/bin/X11:/usr/local/bin:/usr/local/bin
MAIL=/var /spool/mail/wietse SHELL=/bin/csh TERM= xterm (csh)

ps incantations (System V)

 # ps -ef

UID	PID	PPID	C	STIME	TTY	TIME	COMD
wietse	9157	9154	24	12:57:58	pts/0	0:00	-csh
wietse	9184	9157	21	13:00:43	pts/0	0:00	ps -ef

 # ps -ealf

F	S	UID	PID	PPID	C	PRI	NI	ADDR	SZ	WCHAN	STIME	TTY	TIME	COMD
8	S	wietse	9157	9154	25	41	20	fc52bcc0	218	fc52be90	12:57:58	pts/0	0:00	-csh
8	O	wietse	9204	9157	21	55	20	fc52b000	173		13:13:03	pts/0	0:00	ps -ealf

List Open Files and Connections

 # lsof-p 12823 *ftp://vic.cc.purdue.edu/pub/tools/lsof*

COMMAND	PID	USER	FD	TYPE	DEVICE	SIZE/OFF	INODE	NAME
<defunct>	12823	root	cwd	VDIR	7, 22	1024	868362	/var
<defunct>	12823	root	T00	VREG	7, 22	32768	868676	/var
<defunct>	12823	root	T01	VREG	7, 6	24576	139429	/usr
<defunct>	12823	root	T02	VREG	7, 6	516096	139397	/usr
<defunct>	12823	root	T03	VREG	7, 0	4096	14951	/
<defunct>	12823	root	T04	VREG	7, 6	40960	139492	/usr
<defunct>	**12823**	**root**	**3u**	**inet**	**0xff64b50c**	**0x0**	**TCP**	***:5120**

The intruder had left behind a process running with super-user privileges that listened for incoming connections on TCP port 5120. This process looked like a privileged backdoor However, the executable file itself had been deleted.

This slide is intentionally left blank

Section 11

Forensics on Intrusion Activities

529

Reconstruction of User Activity

- Reconstruct what was typed
- Determine what happened
- Determine the damage done
- Determine what files are used
- Correlation is the key

530

What to Trust

- When a machine has been compromised, all information that comes from the machine must be treated with extreme suspicion
- Intruders routinely replace system utilities such as *ls*, *ps* and *netstat* with versions that are modified to hide the presence of backdoor programs

531

What to Trust

- Modifications to application program and data files can be detected relatively easily by comparing the files on the system against a known-to-be-good baseline.
- Toolkits for UNIX achieve stealth by modifying a running OS kernel on-the-fly
- Kernel-level modifications can be much harder to detect

532

Unmistakable Rootkit Signature

- Finds trojan versions of command file
  - *find / -type f -print | xargs md5 >file*
    - *du* (hide sniffer, logs, and configuration files)
    - *ifconfig* (hide sniffer activity)
    - *login* (backdoor)
    - *ls* (hide sniffer, logs, and configuration files)
    - *netstat* (hide intruder network connections)
    - *ps* (hide sniffer process)
- Plus what turns out to be configuration files, programs, and a network sniffer logfile with login/password information.

533

Tools & Methods

- Network sniffing
- Shell history
- Process accounting
- Log files
- MAC times

534

Contents of a Forensic Toolbag

- Statically linked data collection tools
  - *dd, cp, cat, ls*
- Mechanism to get more tools or stash data
  - *ftp*

535

How and What to Grab

- Take the system offline
- Keep track of everything you type or do
- Grab first, analyze later
- Note hardware, software, system configuration
- Automation is necessary (time & consistency)
- Follow order of volatility
- Make copies (including tools) to safeguard them

536

Collecting Evidence

- Gather in order of
  - Memory
  - Unallocated filesystem
  - *netstat, route, arp*
  - *ps*, capture all process data
  - *stat* & MD5 on all files, strings on directories
  - Config, log, interesting files such as *cron, at*

537

List Open Files and Connections

- *lsof* command
  - (vic.cc.purdue.edu/pub/tools/lsof)
  - what files a process executes
  - what files a process accesses
  - what network connections a process uses
  - the current directory
  - the internal inode number
  - the name of the filesystem from which the file originated

538

Processes

- Capture state & binary
  - *ps*
  - */proc*
  - *pcat*
  - *lsof*

539

Disk Stuff

- NFS/Net data handled at server
  - *dd* all filesystems (if possible)
  - *stat* & MD5 all files
  - *strings* on directories
  - Capture logfiles, sys configs, important files
  - Kernel, dumps, corefiles

540

Log files

- Network logs
- TCP wrappers
- Daemon logs
- Programs logs
- Kernel logs
- Accounting logs

541

Freezing an Attacker's Process

- Do not connect to the port
  - Bad things might happen
- Do not terminate the process
  - All information would be lost
- Suspend the process
  - *kill* terminates the process
  - *kill -STOP* suspends the process
  - *kill –CONT* resume the suspended process
- Checking the result
  - *# ps ax|grep T*

542

Program Analysis

- Static Analysis
  - Studies a program without actually executing it
  - Disassemblers, decompilers, source-code analysis tools, *strings* and *grep* commands
  - Can reveal how a program would behave under unusual conditions
  - Impossible to fully predict the behavior of any nontrivial program

543

Program Analysis

- Dynamic Analysis
  - Study a program as it executes
  - Debuggers, function call tracers, machine emulators, logic analyzers and network sniffers
  - Analysis is fast and accurate. However, what you see is all you get
  - Difficult to make a nontrivial program traverse all the possible paths through its code.

544

Program Analysis

- Black Box Analysis
  - Dynamic analysis without access to program internals
  - Only observables are the external inputs, outputs, and their timing characteristics.
  - Can include power consumption and electromagnetic radiation

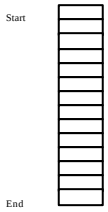
545

Program Analysis

- Postmortem Analysis
  - Study of program behavior by looking at the after-effects of program execution
  - Often the only tool available after system intrusion
  - Some information disappears quickly as normal system behavior erodes away the evidence

546

Process Memory Map



Program code and constants (from program file)
Program variables (saved in core dump)
Direction of growth of stack segment

Shared library code and constants (from lib. files)
Shared library variables (saved in core dump)

Direction of growth of data segment
Stack (saved in core dump)

547

Memory Map

- *# dd < /dev/kmem > output*
- *# dd < /dev/mem > output2*
- *# dd < /dev/rswap > output3*

548

Capturing Process Memory

- *pcat* dumps the entire memory of a process to file, including code, data, heap, libraries and stack

```
# pcat 12832 > pcat.12832
```

To dump all memory of process 12832

- Result can be examined with unstructured tools such as *strings*, binary editor

549

Examining the Memory

- Use *ps* or *lsof* to locate program
  - *pcat* 123 | strings > 123.mem
- *grep* '[host/IP pattern]' 123.mem
- Use *strings* and *less* to examine further

550

File Accessible by Inode Number

- *# ils device*
  - List removed files (inode unallocated and/or refcount 0)
- *# ils -o device*
  - List removed open files (inode allocated but refcount 0)
- *# ils -l device*
  - Existing and removed files (inode allocated/unallocated)
- *# ils device inode*
  - List specific inode
- *# icat device inode >file*
  - Access file content by inode number

551

Capturing Program File

- *icat* retrieves file associated with device name and inode number.
- Recover deleted but still open or running files.

```
# icat <device>/dev/rsd2g 868676 > 868676.out
```

To save contents of file <pid> 868676 on <device> /dev/sd2g

- Result can be examined with standard debuggers and with unstructured tools such as *strings*, binary editors

552

Capturing Process Data

- *gcore* is a standard utility program that takes a snapshot of the process data and stack but not of the program code
- *gcore* creates core dump checkpoints of variables and stack
- *gcore* is not available on LINUX

553

Capturing Process Data

- The output from gcore is in the form of a core dump file
- Result can be examined with standard debugger tools, unstructured tools such as *strings*, binary editors

Core dump checkpoint for process 12832

```
# gcore 12832
gcore: core.12832 dumped
# ls -l core.12832
-rw-r--r-- 1 root 8421808 Feb 24 09:29 core.12832
```

554

Examination with *strings*

```
# strings core.12832 | more
Error: cant open file
kill
Error: cant open file
%s not found
bad port %s
Trying %s...
telcli: socket
:) %s port %d...
csh -bif
exec
pqrstuvwxyzPQRST
/dev/ptyXX
/dev/pty
/dev/ptyp
0123456789abcdef
/bin/csh
/dev/
/dev/tty
fork
/bin/csh
telnetd: %s.
```

Activities of process 12832

555

Capturing Process Information

- /proc filesystem provides process information on executable file, current directory and process memory.
- Entries in /proc/<pid> give access to process info
- Capturing the program file is as simple as copying /proc/<pid>/file
- Capturing process memory requires more work because the memory map has holes in it

556

Capturing Process Information

- Process Attributes

	Solaris	FreeBSD	LINUX
Program file	/proc/pid/object/a.out	/proc/pid/file	/proc/pid/exe
Process memory	/proc/pid/as	/proc/pid/mem	/proc/pid/mem
Memory map	/proc/pid/ap	/proc/pid/map	/proc/pid/maps

557

Capturing Network Information

- All local network states
  - netstat
  - route
  - arp
  - Kernel info
  - Logfiles

558

Remote Network Information

- Speed is important
- Router flow logs
- Portmasters , dialup equipment
- Sniffer, tcpdump
- Server information
  - DNS, NFS, NIS, mail, syslog, WWW, news
- Information gathered for this host
- Telcos
- ISPs
- FIRST/CERTs

559

Watching a Process in Action

- Tracing a process at the machine instruction level generates enormous amounts of information.
  - Tracing process manipulates the traced process via operating-system debugger hooks.
  - Passing control back and forth between the traced process and the tracing process after each machine instruction slows down execution
  - Every file access, every network access, every interaction with the world requires a system call to request assistance from the operating system.

560

Watching a Process in Action

- Use standard debugging hooks to intercept and log
  - System calls (tapping the user-kernel interface)
  - Library calls (tapping the application-library interface)
  - Individual application routines (requires program file)
  - Individual machine instructions
- Run-time tracing can generate large amount of data
- Run-time tracing can impact performance noticeably

561

Watching System Calls

- Watching system calls is better than watching machine instructions
  - System calls happen at much lower frequency
  - Causes less slowdown of execution
  - Produces less information
- Information about system calls
  - Have better signal to noise ratio
  - Suitable for filtering on the function call name or on function call arguments

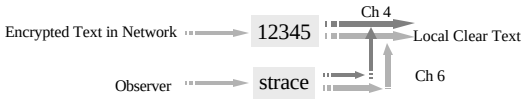
562

Watching System Calls

- User-kernel interface does not show what happens inside the application or inside library routines
- All information must enter or leave the program via a system call, input, output, network, file or terminal
- Many system-specific tools
  - trace (SunOS 4)
  - truss (Solaris 2)
  - ktrace (*BSD)

563

System Call Tracing




```
# strace -p 12345
  -f
  -e trace=read,write
  -e read=6
  -e write=4
```

watch process 12345
and its child processes
show everything read from Ch 6
show everything written to Ch 4
look at read/write calls only

564

Host Based Tracing

- *ltrace*
  - ftp://ftp.debian.org/debian/dists/unstable/main/source/utils/
  - Log every library routine call (output like strace)
  - Portable to LINUX
- *ttywatcher*
  - ftp://coast.cs.purdue.edu/pub/tools/unix/ttywatcher/
  - Real-time monitoring
  - Portable to SUNs
- *tap*
  - ftp://coast.cs.purdue.edu/pub/tools/unix/tap/
  - Hook into streams -based tty systems.
  - Portable to SUNs

565

Hiding a Process from Observation

- Cannot use lots of CPU, memory or I/O resources
- Modified *ps, lsof, top* applications or library routines
  - Can be sufficient when process listing applications must be installed as privileged commands.
- Modified kernel: crude implementations of loadable kernel modules
  - Hides a process even from the most privileged users.
  - http://thc.pimmel.com/

566

Hiding a Process from Observation

- Standard B2+ security feature (covert channels)
- Spying on an intruder without being seen
- Hiding a password sniffer process
- Other forms of surveillance

567

A Forensic Case Example

Investigating a suspected intrusion

- Priorities:
  - Gathering evidence of the break-in
  - Prevent or contain the damages
  - Restore the integrity of the system

568

When Faced with a Situation

- Secure and isolate
- Record the scene
- Conduct a systematic search for evidence
- Collect and package evidence
- Maintain chain of custody

569

Leave the System On / Off ?

- Leave the system running
  - Catching the intruder red-handed
  - Preserving evidence on live connections and RAM
  - Danger of losing or overwriting evidence during investigation
- Disconnect and reboot the system
  - Contain the damage
  - Danger of destroying more evidence

570

Help the Investigator

- Ask all non-essential users to log off
  - To facilitate investigation
  - To reduce noise interference
  - To prevent malicious code from spreading
- Offer use of system administrator account
  - To enable investigator freedom of access for purpose of investigation and gathering evidence

571

Document the Investigation

Open a log file to keep a complete record of all investigation activities

```
# /bin/script evidence
Script started, file is evidence
# date
Sat Mar 6 20:03:34 1999
```

Type *exit* to close log on completion

572

Check Who is On

Your administrator login

```
# /bin/who
root console     Mar 6 16:00
rewt pts/26      Mar 6 15:45      (174-16-52.world.com)
```

Suspected intruder since all other users have log off

Source of intruder's remote access

573

Check Recent TCP/IP Connections

Indications of Telnet connections from world.com to forensic-science.com

```
# /bin/netstat –a
cases.forensic-science.com.telnet 174-16-52.world.com.1711      8235
      0          64260    0          ESTABLISHED
```

Confirms remote connection based on *who* and *netstat* results

574

Check Intruder Logins

Intruder still online

```
# /bin/last rewt
rewt      pts/26   174-16-52.world.com     Sat Mar 6  15:45    still logged in
rewt      pts/5    214-72-229.world.com    Sat Mar 6  00:13 – 00:27 (00:13)
```

575

Determine Intruder Activities

List all intruder's processes

Processes with start time > 24 hrs

```
# /bin/ps –auxwww | grep rewt
UID   PID   PPID  C   STIME   TTY     TIME CMD
rewt  2198  2191  0   Mar 6   ?       378:50 rsh www.corpus-delicit.com
                                      exec/temp/.invisible/destroy
rewt  2186  1993  0   Mar 6   ?       295:31 sniffer
root  4094  3155  0   16:02:14        0:00 grep rewt
rewt  1993  1946  0   15:46:57 pts/24 0:01 -csh
```

Possibly a destruction program running on remote machine www.corus-delicit.comusing remote shell

576

Contain the Damage

Stop the intruder's processes

```
# /bin/kill –9 2198
# /bin/kill –9 2186
# /bin/kill –9 1993
```

PID of processes executed by rwet

577

Trace the Log

```
# /bin/more syslog
Mar 5 23:43:13 cases.forensic-science.com mountd[513]:
  Unauthorized access by NFS cilent 174-16-65.world.com
Mar 5 23:43:13 cases.forensic-science.com syslogd:
  Cannot glue message parts together
Mar 5 23:43:13 cases.forensic-science.com mountd[513]:
  Blocked attempt of 174-16-65.world.com to mount
```

Intruder gained access through a vulnerable version of mountd

578

Trace the Log

Intruder exploited buffer overflow to log in

```
# /bin/more syslog
^E^H ^E^H ^E^H ^E^H ^E^H ^E^H ^E^H ^E^H ^E^H ^E^H
  ^E^H ^E^ ^E^H ^E^H ^E^H ^E^H ^E^H ^E^H ^E
  ^E^H H ^E^H ^E^H ^E^H ^E^H ^E^H ^E^H ^E^H
  ^E^H(Mar 5 23:43:13 cases.forensic-science.com ^E^H
  ^E^H ^E^H ^E^H ^E^H ^E^H
```

Overflow data from a file

579

Trace the Log

File containing buffer overflow data

```
# /bin/more syslog
Mar 5 23:46:54 cases.forensic-science.com PAM_pwdb[3122]: (login)
  session opened by user doomed by (uid=0)
Mar 5 23:46:54 cases.forensic-science.com login[3122]: LOGIN ON
  ttyp0 BY crak0 FROM 174-16-65.world.com
Mar 5 23:50:03 cases.forensic-science.com PAM_pwdb[3130]: (su)
  session opened for user rewt by doomed (uid=0)
```

Switching to a newly created account with root access

580

Determine Intruder Activities

Recall on the intruder's processes

```
# /bin/ps –auxwww | grep rewt
UID   PID   PPID  C  STIME   TTY    TIME    CMD
rewt  2198  2191  0  Mar 6   ?      378:50  rsh www.corpus-delicit.com
                                            exec/temp/.invisible/destroy
rewt  2186  1993  0  Mar 6   ?      295:31  sniffer
root  4094  3155  0  16:02:14        0:00   grep rewt
rewt  1993  1946  0  15:46:57 pts/24 0:01   -csh
```

Look for this program

581

Directory Missing

```
# /bin/cd /tmp
# /bin/ls -altc
drwx--------  2 root  root  512  Mar 6 Jan 1 15:33  ./
drwx--------  8 root  root  512  Jan 1 15:33       ../
```

/tmp/.hidden not found

ls command may have been replaced with a modified version that does not list the hidden directory */tmp/.invisible*

582

How to Hide a Directory

Install the rootkit as follows

```
mkdir .invisible
mv rootkitkit .tar.gz .invisible
cd .invisible
tar zvf rootkit .tar.gz
ls
cd rootkit
./install
exit
```

583

RedHat Package Manager (RPM)

- The RPM provides a convenient way to determine if common system files like *ls* have been modified
- The command *rpm –Va* verifies all of the important files on the system
- This method is not failsafe
  - A sophisticated intruder can also modify the RPM database to hide changes made to the system

584

List All Subdirectories

Surely enough, the version of *ls* has been modified

```
# /bin/du
10273 ./.invisible
10273
```

The originally hidden subdirectory

585

Examine Intruder Activities

Hidden subdirectory

```
# /bin/cd  /tmp/.invisible
# /bin/ls –altc
-rw-r--r--  1  rewt  3925716  Mar 6 21:21  info3
-rw-r--r--  1  rewt  108133   Mar 6 16:48  info2
-rw-r--r--  1  rewt  1818708  Mar 6 16:03  info1
-rw-r--r--  1  rewt  4414846  Mar 6 15:54  destroy
drwxr-xr-x  2  rewt  512      Mar 6 00:22  sniffer
drwxr-xr-x  3  rewt  512      Mar 6 00:20
drwxr-xr-x 393 root  7168     Jan 1 15:33
```

586

Follow Up

- Terminate the script logging the investigation by typing *exit*
- Print all evidence and sign on each page
- Copy evidence to disk using *tar* (instead of *cp*) to preserve timestamps and file attributes
- Create message digest for each digital evidence

587

Follow Up

- Duplicate evidence for safekeeping and further investigation
- Reboot the system
- Make a bitstream copy of the hard drive
- Examine router log files
  - Log files will reveal trial and error entries of intruder attempting to gain access
- Reformat disk, reinstall OS
- Issue new passwords to all users

588

Post-Mortem

- Intruder had
  - Exploited common vulnerability to intrude into system
  - Obtained access from a dial-up account at world.com
  - Modified the system using a rootkit
  - Created a hidden directory by modifying ls
  - Hide tools in hidden directory

589

This slide is intentionally left blank

590

This slide is intentionally left blank

591

This slide is intentionally left blank

592

This slide is intentionally left blank

593

This slide is intentionally left blank

594

Section 12

Forensics on Wireless Network

595

Wireless Network Analysis

- The ubiquitous nature and increasing complexity of wireless networks raises a host of criminal and legal issues.
- Of concern is how law enforcement can locate and process wireless network digital evidence and ensure that it is legally admissible.

596

Wireless Network Analysis

- Time is of the essence when collecting data. It is important to build relationships and procedures with wireless operator personnel so that when a situation arises, time will not be lost.
- The list on www.infobin .org has the names of ISPs and contacts at their legal departments for services of court orders and search warrants.

597

Wireless Network Analysis

- Generally, the most complex parts of the process are
  - Law enforcement having to find the right people to talk to at the wireless network operator.
  - The system analyst receiving authorization to track a phone call.

598

Wireless Network Analysis

- The ability to quickly track a subscriber location during the course of a phone call is possible but requires personnel familiar with the network operator's equipment.
- Procedures should be in place at the operator to aid in rapidly expediting the investigation.
- Procedures should also be in place for law enforcement so that they know who to call for emergency assistance.

599

Circuit Switched Wireless Network

- The 3 most popular digital circuit switched wireless technology
  - GSM
    - Global System for Mobile Communications, TDMA
  - IS-136/TDMA
    - Time Division Multiple Access
  - IS-95/CDMA
    - Code Division Multiple Access

600

Mobile Device

- A GSM mobile device is marked with a unique International Mobile Equipment Identity (IMEI) numbers.
- IS-136 and IS-95 mobile devices are marked with a unique ESN (Electronic Serial Number).
- The IMEI or the ESN can be found printed on the back of the mobile device.

601

Mobile Equipment Identity

- The 14 digits IMEI contains the
  - Type Approval Code (TAC)
    - 6 digits
    - Issued by the certification body to the manufacture
  - Final Assembly Code (FAC)
    - 2 digits
    - Issued by the manufacture for this particular equipment type
  - Serial Number (SN)
    - 6 digits
    - The manufacturer's unique production number

602

Mobile Equipment Identity

- The IMEI can be interrogated with the key combination *#06#.
- A 1-digit Check Digit (CD) is calculated from the 14 IMEI digits and is not sent within the GSM network.

603

Mobile Equipment Identity

- The IMEI can usually be found in the EEPROM memory.
- There are many tools available for modifying the IMEI. This may provide problems when tracing and furnishing proof on the use of the mobile device.

604

SIM Card

- In GSM, the Subscriber Information Module (SIM) contains data such as
  - The subscriber's phone number
  - The subscriber identity number
  - The subscriber's PIN number
  - Authentication keys

605

SIM Card

- The phone number is called the Mobile Subscriber ISDN.
- The International Mobile Subscriber Identity (IMSI) is globally unique to a particular subscriber. The 15 digits IMSI can indicate the subscriber's country and wireless network operator.

606

SIM Card

- A Temporary Mobile Subscriber Identity (TMSI) can also be stored on the SIM card to avoid revealing the IMSI number.
- IS-136 and IS-95 mobile device do not use a SIM card. The phone number or Mobile Identification Number (MIN), the IMSI, PIN number and authentication keys reside on the mobile device itself.

607

SIM Card

- Data in a SIM is protected with a PIN.
  - The number of attempts at entering a PIN is limited to 3.
  - If none of the attempts is successful, access to the protected data is blocked.

608

SIM Card

- This blockade can be lifted with a PUK (Pin Unblocking Key).
  - A PUK is entered together with a newly chosen PIN.
  - The number of attempts at entering a PUK is limited to 10.
  - In many countries, PUKs can be obtained from the subscriber's network provider.

609

Extraction of SIM Data

- Cards4Labs (www.forensischinstituut.nl) is modular program for reading smart cards via PC/SC compatible smart card readers.
- For reading SIM data, the PUK can be requested from the network provider with relevant authorization.
- This PUK, when entered with a PIN of choice, allows access and decoding of files, including data that have been erased.

610

GSM Memory

- It is also possible to retrieve supplementary data through the direct reading of the EEPROM or FLASH memory contained in the GSM device.
- To do this, the memory is removed and read with a universal programming device.
- The decoding process amounts to looking at the memory dump in a hexadecimal viewer such as the Hex-Workshop (www.hexworkshop.com).

611

Back Door

- Many systems have a back-door deliberately built in to circumvent security.
- The reserve password may be found in the technical documentation.
- For some GSM, service sets used by repair departments can be used to retrieve or circumvent these device passwords.

612

Mobile Switching Center

- The MSC is the nerve center of the circuit switched network.
- The MSC performs call setups and maps out the path of a call between the originating and destination points.
- The MSC switches calls between Location Areas and between other MSCs .

613

Mobile Switching Center

- The MSC interconnects calls from its own network area to other fixed line network, a data network, or another wireless network.
- Billing information in the CDR (Call Detail Record or Charging Detail Record) is also derived from the MSC.

614

Home Location Registry

- The HLR contains subscriber information such as who pays the bill, their billing address, their phone number, the services that they are allowed to use.
- The HLP will always know the location of the mobile device as it may need to route call to the mobile device.
- Ciphering keys for a particular subscriber are also held in the HLR.

615

Visitor Location Registry

- The VLR contains the subscriber information of all users active in a particular MSC's network.
- When a subscriber roams into a new MSC area, the VLR will request information from the subscriber's HLR and create a record for the subscriber.

616

Visitor Location Registry

- At the same time, the HLR will create a record showing the name of the VLR to which a subscriber is presently associated.
- When the subscriber moves out of an MSC's area, the record in the MSC's VLR is created and the HLR is notified.

617

Equipment Identity Registry

- In GSM, the EIR contains a list of IMEI numbers that the operator has registered. The EIR can be used to blacklist stolen mobile devices to prevent further abuse.
- IMEIs are categorized as
  - White: authorized mobile devices
  - Black: unauthorized/reported stolen mobile devices
  - Gray: malfunctioning mobile devices.

618

Operational and Maintenance Center

- The OMC provides a view of the operational status of the network, network activity and alarms.
- The OMC can be used to
  - collect traffic information from the network
  - examine a particular mobile call in progress (mobile trace)

619

Turning on a Mobile Device

- Switching on a mobile device causes the device to register with the network and inform the network of its Location Area.
- The mobile device may also be requested to perform a location update every so many minutes to identify its location within the network.

620

Turning on a Mobile Device

- The MSC for the area informs its VLR as to the Location Area the mobile device has reported its presence and inform the subscriber's HLR accordingly.
- Information from the subscriber's HLR will also be updated with the VLR name with which the subscriber is now registered.

621

A Mobile Device in Idle State

- In a listening state, the mobile device may be asked to perform a Location Area update.
- This allows the network to identify the Location Area in which the subscriber resides.

622

Roaming with a Mobile Device

- With the information exchange on the Location Area, the subscriber's home network will know the wireless network operator and MSC/VLR where the subscriber is roaming, either in
  - The home network
  - Another network
  - A network in another country

623

Connecting A Call

- When placing or receiving a call with a mobile device, the network knows which cell sector to which the subscriber is connected.
- This particular location information is transient (possibly 72 hours or less) as compared to the information such as the calling party and called party, which can be found in most billing records.

624

Areas of Digital Evidence

- Areas useful for forensics on wireless network:
  - Equipment connected to the mobile device
  - The mobile device itself
  - The wireless network
  - The subsequent network that the caller accesses

625

Equipment on the Mobile Device

- Criminal activity involving wireless networks can involve a laptop connected to a mobile device.
- Data that may prove useful to an investigation may reside on the laptop or network.

626

Equipment on the Mobile Device

- A laptop enabled by a mobile device may have been connected to a Ethernet or wireless (802.11) network.
- If a mobile device has then been used to dial-up to another network, then the laptop may contain useful data (time, numbers dialed, session logs).

627

The Mobile Device

- Many mobile devices have some sort of PIM (Personal Information Manager) built into the device that may yield useful information.
- The mobile device memory (and the SIM card) may contain critical information.

628

The Mobile Device

- The phone lists within the mobile device may contain: received call phone numbers, dialed phone numbers and missed phone numbers stamped with a data and time.
- Do not assume that the date and time are accurate on a mobile device. The subscriber may not have taken care to set the time exactly.

629

The Mobile Device

- Most mobile devices have the capability to store names and phone numbers for a subscriber to dial.
- This information may also yield valuable information, such as names and numbers of people the subscriber communicates with regularly.

630

The Mobile Device

- The mobile device memory (and the SIM card) can also hold other data of interest:
  - Location information
  - Administrative data
  - Ciphering keys
  - IMSI
  - MSISDN (phone number) for subscriber identification
  - Correlation to billing record
  - Location where the mobile device was last used.

631

The Mobile Device

- The mobile device may also hold voicemail number, voicemail PIN, numbers stored on speed dial and calling card information.
- SMS messages of interest may still be resident on the mobile device or SIM card. The inbox stores incoming SMS messages, while the outbox or sent lists contain previously sent SMS messages.

632

The Mobile Device

- Mobile devices may also use PIN numbers that may hamper access to data resident in the mobile device.
- When seizing mobile device, losing power, running out of battery power, or removing the battery, could cause the irretrievable loss of information.

633

The Wireless Network

- The MSC can be rich with digital evidence.
- Billing records can contain the caller's number, receiving party number, time when the call was placed, and duration of call.
- Billing records may also note how and when payment was executed.

634

The Wireless Network

- The HLR contains subscriber information that can be matched to a phone number.
  - It is important to know that not all GSM network operators use EIRs.

635

The Wireless Network

- SMS messages may be kept for a varying period of time at the SM-SC (Short Message Service Center)
  - Messages for a particular subscriber may be waiting here, ready to be forwarded.
  - These waiting unclaimed messages could be valuable for the investigator.

636

The Wireless Network

- The OMC and the signaling links can provide data in real time regarding the activities of a subscriber.
- Due to the extensive capabilities of the OMC, user activities of network operator personnel should be logged. These logs may also be useful.

637

The Wireless Network

- The elements in the core network interface with each other via the SS7 (Signaling System #7) protocol.
- Logging SS7 data can yield information regarding mobile location or evidence indicating wireless subscriber fraud such as cloning.

638

The Subsequent Network

- The caller may use a mobile device to accessed a subsequent network.
- If one network hands off to the other network, a record will be kept. This can be useful for determining a suspect's activity near a border between countries roaming.
- However, the MSC may be in a different country and information from the foreign operator may not be readily available.

639

Concerns with Encryption

- Most wireless technology standards emphasize security of the radio link but do not provide for real security on the core network where communications and signaling takes place.
- Information is not encrypted after the BTS (Base Transceiver Station). Easier to wiretap the non-radio links at the MSC rather than the radio link itself.

640

Concerns with Encryption

- Wiretapping at the MSC is the easiest method to obtain unencrypted information.
- Cipher keys and authentication values used by mobile devices to encrypt communications are passed in clear text between MSCs .

641

Records kept in the MSC

- The MSC is the heart of the network.
  - It stores everything internally in memory and releases these data as input to other functions in the switch.
- Records collected by the switch pertain to
  - Billing
  - Fraud management
  - Security
  - Network operations

642

Billing

- Billing records are usually kept in a database for use by customer service.
- Billing data are typically archived for a long term, such as 7 years for both legal reasons and to monitor customer behavior over time.

643

Billing

- The anchor switch which routes a call from a mobile device is tasked for
  - Generating its own CDR (Charging Details Records)
  - Collecting CDR from other switches through which the call passes

644

Fraud management

- The fraud management system analyzes the CDR for unusual and abnormal patterns.
- The fraud management system will note when a subscriber breaks this pattern and if this unusual activity continues for a period of time.
- The network operator may then call the subscriber to ensure that the mobile device is under the subscriber's control.

645

Wiretapping

- A judge may issue a court order demanding that a particular phone number of a suspect's mobile device be wiretapped.
- The security department at the network operator can then authorizes a wiretap to be performed by its technical personnel.

646

Wiretapping

- When the subscriber's mobile device makes a call or receives a call,
  - The operator's switch will break out a second line for the call
  - The second line is then passed over a secure connection to the law enforcement personnel concerned.

647

Network Operation Data

- Network operation details can quickly take up massive amounts of storage space.
- Records are soon aggregated into smaller summary files to save storage space, and to focus operator personnel on higher priority issues e.g. dropped calls.

648

Network Operation Data

- A phone call can pinpoint (down to the cell site) where the call was made from.
- However, after the operational network data are summarized, only the switch name associated with the call will be available.

649

Location Based Services

- Various types of position determining equipment (PDE) technologies exist to calculate the location of a subscriber down.
- Using these technologies, a wireless operator can provide to its subscribers location based services.
  - For instance, a message or advertisement could be sent to the subscriber's mobile device about local attractions or services.

650

Location-Based Services

- Using position determining equipment, a mobile can also be 'pinged', thus
  - Forcing the mobile to re-register with the network
  - Provide signals for the position determining equipment to home in and fix a location

651

Location-Based Services

- Position determining technologies can also enable an operator to provide emergency services.
- When an emergency call is placed, the operator may be able to locate the position of the subscriber.

652

Wireless LAN Technology

Specifications	Speed	Frequency	Techniques
802.11	< 2 Mbps	2.4 GHz	Freq Hopping Spread Spectrum Direct Seq Spread Spectrum Infrared
802.11a	< 54 Mbps	5 GHz	Orthogonal Freq Div Multiplex
802.11b	< 11 Mbps	2.4 GHz	Direct Seq Spread Spectrum

653

Wireless LAN Analysis

- Areas useful for forensics on wireless LAN:
  - Equipment connected to the mobile device
  - The mobile device itself
  - The wireless network
  - The subsequent network that the caller accesses

654

Equipment on the Mobile Device

- A laptop connection enabled by a WLAN card may be connected to an 802.11 network. Software in the PC may contain useful data of network activity.
- The network to which a WLAN user is connected to may also contain session logs of the user's activity within the network.

655

The Mobile Device

- Like the Network Interface Card on the Ethernet, the WLAN card has a fixed Media Access Control (MAC) address that is unique to the WLAN card and can also be used to identify the card 's vendor.
- The MAC address of the WLAN card can provide a form of identification of the mobile device used in the wireless connection.

656

The Wireless Network

- Access Point on the wireless network logs associations based on the MAC address. Most Access Points allow administrator to configure an access list based on MAC address.
- The Dynamic Host Configuration Protocol (DHCP) server then issues IP addresses to the WLAN users.

657

The Wireless Network

- An intruder can jump in and join a network for which he does not have permission to join by using a probing mechanism.
- Such probing mechanism permits a broadcast request to gather Access Point information and then carry out an auto-join function into the network.

658

The Wireless Network

- Access Points should have the ability to support encryption using Wired Equivalent Privacy (WEP).
- Even when the WEP is enabled, the Network and MAC information always passed in clear-text.

659

The Subsequent Network

- The subsequent network may contain session logs of the user's activity within the network.
- Digital evidence in this area can be extremely difficult to access, particularly if the evidence is in another country.

660

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX F: HANDOUTS FOR LABORATORY EXERCISES

The following pages, 1 – 16, are the handouts for the laboratory exercises.

Forward

This set of laboratory exercises is specially designed to illustrate the computer forensic concepts being taught in class. By performing the exercises, it will help you to understand and internalize the key concepts. In these exercises, you will learn to use operating system tools and rootkits to extract useful digital evidence as well as lay your hands on professional computer forensic software and freeware.

The intention of this laboratory manual is not to spoon-feed you with step-by-step instructions on how to conduct a forensic examination. Rather, you will be expected to actively search for the relevant information, user instructions and downloads, in carrying out your exercises. This is to build up your resourcefulness and creativity towards tackling future forensic examinations. Pertinent technical guidance will accompany each of these exercises in order to help you get started.

Do not attempt to copy from the forensic examination of other project groups, as each group will be issued with subject evidence with subtle differences among them.

Maximize the use of the technical resources available in the laboratory and make this an enjoyable learning experience. Good luck.

Contents

Laboratory Exercise 1: Foundstone Forensic Toolkit……3

Laboratory Exercise 2: EnCase (Guidance Software)..……..5

Laboratory Exercise 3: AccessData Forensic Toolkit..…….……..8

Laboratory Exercise 4: Windows Event Log Analysis..……...…..10

Laboratory Exercise 5: DumpEvt (SomarSoft)..……..12

Laboratory Exercise 6: Unix Log Analysis..……...……...…..14

Laboratory Exercise 7: Network Analysis..……..……..16

Laboratory Exercise 1: Foundstone Forensic Toolkit

Introduction

The Foundstone Forensic Toolkit contains several Win32 command line tools to help examine files on a NTFS disk partition for unauthorized activity. Some of these open source tools include

AFind lists files by their last access time without tampering the data the way that right-clicking on file properties in Windows Explorer will. *AFind* allows you to search for access times between certain time frames, coordinating this with other logon information, you can determine user activity even if file logging has not been enabled.

HFind scans the disk for hidden files. It will find files that have either the hidden attribute set, or NT's unique and painful way of hiding things by using the directory/system attribute combination. This is the method that Internet Explorer uses to hide data. *HFind* lists the last access times.

SFind scans the disk for hidden data streams and lists the last access times.

FileStat is a quick dump of all file and security attributes. It works on only one file at a time.

Technical Guidance

1. You should be able to obtain the necessary information and downloads from the knowledge page at www.foundstone.com to install the forensic software on your forensic PC. If you need specific technical assistance on the Foundstone Forensic Toolkit, you may contact labs@foundstone.com. The web page provides valuable information on the command line switches for the various embedded tools.

2. You will need to first unzip the downloaded file before installation.

3. You will also be issued a duplicate of the subject floppy disk you are going to examine.

4. Open a DOS Command Prompt to run the forensic tools. You may also explore with the other tools in the Foundstone Forensic Toolkit that are not described above. You can type the name of the tools to list the command line switches that are applicable to them.

5. Run *Afind* with the correct command line switch to determine files which were accessed within the last 2 days.

6. Run *Hfind* with the correct command line switch to determine the last access time of the hidden files.

7. Run *Sfind* with the correct command line switch to determine the last access time of the hidden data streams.

8. You may also use *FileStat* to perform a quick dump of all the content and security attributes of the files you have examined above (one at a time) to your evidence file.

9. Compare the above findings with that using the *dir* command in DOS. What are the command line switches required in *dir* to generate the equivalent information?

Laboratory Exercise 2: EnCase (Guidance Software)

Introduction

EnCase is the industry leading computer forensic software tool used by most all computer forensic examiners. Award winning and court tested, EnCase software allows law enforcement and IT professionals to conduct a powerful, yet completely non-invasive computer forensic investigation. EnCase features a graphical user interface that enables examiners to easily manage large volumes of computer evidence and view all relevant files, including "deleted" files, file slack and unallocated data. The integrated functionality of EnCase allows the examiner to perform all functions of the computer forensic investigation process, from the initial "previewing" of a target drive, the acquisition of the evidentiary images, the search and recovery of the data and the final reporting of findings, all within the same application. The final reports and extracts generated by the built-in report feature documents the investigation results and integrity of the original data with a clear and concise chain of custody to ensure the authentication of the examined electronic evidence in a court of law.

Requirements

1. Installation of the forensic software
2. Acquisition of evidence from the subject PC
3. Creation of evidence files for forensic analysis
4. Analysis of acquired evidence
5. Recovery of deleted files and folders
6. File signatures analysis
7. Hash value analysis
8. Temporal reconstruction of events
9. Creation of forensic report
10. Presentation of forensic analysis in class (20 min)

Technical Guidance

1. You should be able to obtain the necessary information and downloads from www.encase.com to install the forensic software on your forensic PC. If you need specific technical assistance on EnCase, you may contact support@encase.com or help@encase.com, or go to the technical support web page. The web page provides valuable information on setting up, acquisition, analysis, archive, restoration, reporting and other technical support.

2. You will be issued with a physical dongle in order for EnCase to run on your machine—a copyright protection feature. Attach the dongle onto your machine's USB or parallel-port. You will also be issued with a user name and password to enable you to perform download from the EnCase website.

3. Download EnCase from the website to your Windows-based forensic PC (the computer used to conduct the forensic examination). Run setup.exe and install EnCase. Reboot your PC.

4. Run EnCase. Goto the Tools menu to create an EnCase boot disk. The boot disk is used to boot up the subject PC (the computer you are going to examine). It can also be used to boot up your forensic PC to a safe version in DOS.

5. Connect the subject PC directly to your forensic PC using either the lap-link parallel cable or network cross-over cable. In order to connect to the forensic PC on the network cable, ensure that the subject PC has a NIC supported by EnCase in the boot disk. You may also need to disconnect your forensic PC from the LAN if there is only one NIC on the machine. The list of supportable NIC can be found on www.encase.com/html/encase_network_boot_disk_page.htm. Otherwise, get the DOS packet driver for the specific NIC on the subject PC, copy and load (may require creating a config line in a batch file) the packet driver on the boot disk.

6. Boot up the subject PC using the EnCase boot disk. Load the packet driver and launch EnCase for DOS.

7. Boot your forensic PC into Windows, launch EnCase for Windows. You should be able to preview and acquire evidence on the subject PC from your forensic PC.

8. Preview the subject PC. This feature is designed to allow you to pre-scan a suspected drive for potential evidence efficiently. As an exercise, you will not need to acquire the entire drive in the subject PC to your forensic PC for analysis—this will take too much memory, even if compressed, and too much of your time. You will just have to do a screen capture on a preview of the subject PC to show that you know how to preview and acquire evidence remotely.

9. Explore the various functionalities of EnCase.

10. Assuming the evidence is already captured on a floppy disk this is issued to you. Insert the floppy disk onto your forensic PC and acquire the evidence on the local disk. Create an evidence file of the subject floppy disk.

11. You may also want to add external viewers (e.g. add MSWORD.EXE to for .doc files or OUTLOOK.EXE to for email messages) to EnCase to help view the data stream in the files more easily.

12. Print out your certification of completion. Hint: It is a file attachment within another file that has been deleted in a hidden folder. Note the original file type may have been changed.

13. Proceed to analyze and document your findings on the evidence file into a report. Perform the relevant steps to fulfill the laboratory requirement stated above.

14. Summarize your forensic investigation and make a presentation of your case in a legally convincing manner in class.

Laboratory Exercise 3: AccessData Forensic Toolkit

The AccessData Forensic Toolkit (FTK) is a handy utility for computer crimes investigators. FTK offers users a complete suite of technologies needed when performing forensic examinations of computer systems. Its full text indexing offers quick advanced searching capabilities. Its deleted file recovery and file slack analysis are commendable. FTK is also interoperable with AccessData's password recovery and encryption file identification programs. In addition, the FTK incorporates Stellent's Outside In Viewer Technology to access over 255 different file formats. The Known File Filter (KFF) feature can be used to automatically pull out benign files that are known not to contain any potential evidence and flags known problem files for the investigator to immediately examine. FTK can also support evidence files acquired by EnCase, Snapback, SafeBack and Linux DD.

Requirements

1. Installation of the forensic software
2. Acquisition of evidence from the subject floppy disk
3. Creation of evidence files for forensic analysis
4. Analysis of acquired evidence
5. Recovery of deleted files and folders
6. File signatures analysis
7. Export of recovered deleted files and attachments
8. Creation of forensic report
9. Presentation of forensic analysis in class (20 min)

Technical Guidance

1. You should be able to obtain the necessary information and downloads from www.accessdata.com to install the forensic software on your forensic PC (the evaluation version is adequate for this laboratory exercise). If you need specific technical assistance on the AccessData Forensic Toolkit, you may obtain online support from its web page.

2. You will need to first unzip the downloaded file before installation.

3. You will also be issued a duplicate of the subject floppy disk you are going to examine, assuming the evidence is already captured on a floppy disk.

4. Insert the floppy disk onto your forensic PC and acquire the evidence on the local disk. Create a new case. Adopt the default case log options, processes, case refinements and index. Add evidence and select the local drive of the floppy.

5. Explore the various functionalities of FTK.

6. Recover and export your certification of completion. Print the certificate using the original Microsoft Office application. Hint: You may use the impressive advanced searching capabilities of FTK with the keyword ‘certificate’.

7. Proceed to analyze and document your findings on the evidence file into a report. Perform the relevant steps to fulfill the laboratory requirement stated above.

8. Summarize your forensic investigation and make a presentation of your case in a legally convincing manner in class.

Laboratory Exercise 4: Windows Event Log Analysis

Introduction

Microsoft WinNT/2K can be configured to log events in binary files, namely the

a. System events in *SysEvent.evt*. The system log includes events in the system's operation such as a failed or successful driver startup, an application crash or errors associated with data lost.
b. Application events in *AppEvent.evt*. The application log is for events recorded by applications.
c. Security events in *SecEvent.evt*. The security log contains information such as logon and logoff events, file manipulation, and other resource access events.

Window NT/2K event log stores the descriptive messages in the registry and the separate executables (.exec) or dynamic link library (.dll) files. The Event Viewer combines and displays the information in these files, providing a convenient way to view the data. Consequently, copying event log (.evt) files from one system to another for examination may result in misinterpretation when viewing event logs on a remote system. The Event Viewers will read the event record data from the remote log files, but will search the registry of the local system for the corresponding event message files. Unless the forensic PC have similar configuration to the imaged system, it may be necessary to extract all the registry keys and event message files from the image. By viewing the extracted logs using the Event Viewer, it is possible to create a short list of missing event message files and configure them in the forensic PC accordingly. Otherwise, the Event Viewer will not display explanatory material for any event for which there is no associated event message file.

Requirements

You are the System Administrator of a computer laboratory. It was reported to you that there was an intrusion originating from a Windows NT/2K machine in the laboratory. You are to examine the event logs on that machine with minimal disturbance to the logs that are continuously running on the machine. As such, you decide to extract the event logs and examine them using the Event Viewer on your forensic PC. Trace the security breaches recorded in the event log.

Technical Guidance

1. Extract the event logs and registry keys from the subject PC
   a. Copy the event log (.evt) files from *C:\WINNT\system32\config*
   b. Run *regedit*
   c. Select *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog*
   d. Select menu *Registry>Export Registry Files*

2. Disable the current event logging on the forensic PC
   a. Right click *My Computer* on the desktop and select *Manage*
   b. Open *Services and Applications\Services\Event Log*

c. Select and apply *Disabled* under Startup Type
d. This is necessary because when the event logging service does not shut down cleanly, the Windows Service Control Manager does not reset several bit values that indicate the files is open and thus cannot be accessed. The Event Viewer will report that the file is corrupted and will refuse to open it. However, the log is rarely corrupted in reality.
e. Reboot the PC to apply the selected setting
f. Right click *My Computer* on the desktop and select *Manage*
g. Open *Services and Applications\Services\Event Log*
h. Check that the event log is not started
i. Rename the event log (.evt) files in *C:\WINNT\system32\config*

3. Load the extracted event logs and registry keys onto the forensic PC
   a. Copy the extracted event log (.evt) files into *C:\WINNT\system32\config*
   b. Right click *My Computer* on the desktop and select *Manage*
   c. Open *Services and Applications\Services\Event Log*
   d. Select and apply *Manual* under Startup Type
   e. Start the event log services
   f. Run *regedit*
   g. Select *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog*
   h. Select menu *Registry>Import Registry Files*

4. Load the event message files onto the forensic PC
   a. Examine the data portion of each sub-key for *EventMessageFile* to reveal the path and file name of the file the Event Viewer uses to display explanatory text for each event. Since this is a tedious process, this exercise will be limited to the Security sub-keys only.
   b. Extract these required executables (.exe) or dynamic link library (.dll) files from the subject PC and load them onto the forensic PC.
   c. Double click on the *EventMessageFile* to edit the path and file name of the registry (.reg) files such that it points to the location of the appropriate extracted files on the forensic PC.

5. Analyze the extracted event logs on the forensic PC
   a. Right click *My Computer* on the desktop and select *Manage*
   b. Select *Services and Applications\System Tools\Event Viewer*
   c. This will display the logs from the subject PC, but will add new events to the log files stamped with the current date and time. You may minimize such contamination by immediately generate new copies of the event logs using the Event Viewer's *Save As* command.
   d. If you saved the event log with another file name, you may open the event log file using the *Action\Open Log File* menu option with the Log Type set to the corresponding type.

Laboratory Exercise 5: DumpEvt (SomarSoft)

Introduction

It was evident from the previous exercise, the clumsiness of performing manual Windows event log analysis on a remote forensic PC. Moreover displaying the logs using the Event Viewer is not very conducive for analysis since the Event Viewer is not integrated with other data processing tools. Even Microsoft recommends using the SomarSoft's DumpEvt utility to dump contents of the event log into other formats suitable for spreadsheets and databases. Besides, performing separate log analysis on individual machines in a networked environment does not readily link a related event across multiple machines. Rather, importing the contents of multiple machines' log files into a spreadsheet makes it easier to sort events chronologically and search the logs simultaneously.

SomarSoft's DumpEvt is a Windows NT program designed to dump the event log in a format suitable for importing into a database. It is similar to the DUMPEL utility in the NT resource kit, but without some of the limitations. DumpEvt has also been updated to allow dumping of Windows 2000 event logs containing DNS, File Replication and Directory Service.

Requirements

You are to investigate an intrusion originating from a Windows NT/2K machine in the network. In particular, it was reported that an intruder has remotely installed a Trojan client from machine A onto machine B on the same network. You are to install and use DumpEvt to examine the event logs on these machines to trace the security breaches recorded in their event log.

Technical Guidance

1. You should be able to obtain the necessary information and downloads from www.systemtools.com/somarsoft to install the event log dump utility on your forensic PC. The embedded Help menu provides valuable information on installation, command line options, known bugs and limitations, and other technical support.

2. You will need to first unzip the downloaded file before installation.

3. Use the Notepad to create a batch (.bat) file to extract the event logs from machine A and machine B onto the forensic PC.

   For example, the following command lines will extract the whole (*all*) application log (*app*) from both the subject PC (*machine A, machine B*), and append them to (or create new) an output file (*c:\evidence\application_log.csv*) on the forensic PC, in a comma-delimited spreadsheet (*.csv*) that can be viewed on Excel. The status and error messages of the extraction are appended to a text file (*c:\evidence\error.txt*).

   dumpevt.exe /computer=***machine_A*** /logfile=***app*** /outfile=***c:\evidence\application_log.csv*** /all >> ***c:\evidence\error.txt***
   dumpevt.exe /computer=***machine_B*** /logfile=***app*** /outfile=***c:\evidence\application_log.csv*** /all >> ***c:\evidence\error.txt***

4. Run the batch file.

5. Open the output files using a spreadsheet to facilitate your analysis.

Laboratory Exercise 6: Unix Log Analysis

Introduction

Unix serves as a wonderful training ground for computer security specialists. It teaches about access permissions for objects; learning about those rwx's in directory listings gives one an appreciation for granular security. It builds on MS-DOS knowledge: hidden files are dot files in Unix. They become visible by the *ls-al* command (similar to *dir /a:h*). Unix expands on MS-DOS piping and redirection capabilities. Searching or manipulating files and directories using *find* and *sort*, an investigator, for example, can search a directory for inactive files (by date) and pipe the results into a report file. The *find* command also produce a comprehensive list of files with the SUID/SGID permission set. Using Unix scripting capabilities (similar to DOS batch files), an investigator may create combinations of commands into specialized programs to conduct security audits and to do file checking as a part of an inquiry. The *grep* command searches files or directories that contain a particular character string. This capability provides for granular searching. Unix also has the capability to list processes actively running on the machine by executing the command *ps -ef*. Processes may be deleted using the *kill* command. The *top*, *head*, and *tail* commands allow examination of portions of logs or process lists.

The Unix system also has a comprehensive set of system configuration files that can prove to be an invaluable source of information to an investigator. The */etc/syslog.conf* file sets the facility and priority level of individual logs. Some Unix services are specifically initiated or terminated based upon the configuration of scripts located in the */etc/rc* directories. The investigator can get an idea of what services are launched by understanding the Unix scripting and services. Other services are initiated when needed by a daemon that listens for requests. For example, the Internet Daemon is controlled by */etc/inetd.conf* and this file provides the name of the service, the type of delivery, protocol, wait status, UID, server and any arguments. The */etc/passwd* file identifies the properties of the user accounts while password hashes are commonly protected in the */etc/shadow* files. Since UID 0 should be reserved for root only, any other shared UID 0 would ring a bell, so is a 'nobody' daemon account that references a user shell. Scheduled jobs planted by intruders can be found in */etc/cron.d*. The *syslog.conf* configuration file can be used to identify logs with unique names and locations.

Last but no least, the Unix system has a set of standard logs, which include

a. *wtmp/wtmpx* keeps track of login and logouts. Grows in length and is extended to *wtmpx*. This file can be referred to by the *last* command.
b. *utmp/utmpx* keeps track of users currently logged into the system. This file can be referred using the commands *w*, *finger* and *who*.
c. *lastlog* keeps track of each users most recent login time and records their initiating IP Address and terminal.
d. *sulog* records the usage of the *su* switch user command.
e. *httpd* tracks originating IP address of WWW connections.
f. History files keeps a record of recent commands used by the user in the *$HOME* directory.
g. FTP Logs.xfr maintains extensive logs to track incoming connections and the originating IP address of the connection.

h. *maillog* provides status of mail handling.
i. *aculog r*ecords the username, time, date and phone number of dial out facilities.
j. *acct/pacct* maintains a list of user's commands and their process time they used.
k. Packet sniffer logs captures network IP packets.

Requirements

You are the System Administrator of a Unix network server. It was reported to you that there are still system activities originating from the user account *CISR* in the past 1 week, although the particular employee with the above account UID has already left the organization for good. Using the rudimentary Unix commands, system configuration files and standard system logs, trace the activities associated with the user account *CISR* in the past 1 week.

Technical Guidance

1. You will need to log in the Unix system as a System Administrator with root access privileges in order to access the system configuration files and system logs.

2. It will be helpful to pipe and redirect the system configuration files and standard system logs to temporary files before using commands such as *grep*, *find* and *sort* to search or manipulate the files and directories for records with keyword *CISR*.

Laboratory Exercise 7: Network Analysis

Introduction

Analyzer is a fully configurable network analysis program for Win32 environment. It captures packets from network and displays them through a graphical interface. The user can choose the network adapter used for the capturing and monitoring process, specify an appropriate filter, select, copy and paste packets. This product is developed by the Politecnico di Torino and its contributors. It is released under a BSD-style license and partially sponsored by Microsoft Research. *Analyzer* can display the capture files created by *WinDump* and *tcpdump* if the capture files have the ACP extension.

Requirements

You will be issued a set of ACP files with the network traffic captured by *WinDump*, *tcpdump* or *WinPcap* (www.netgroup.polito.it). You are to download and use *Analyzer* to examine the network traffic. Investigate the websites visited by the user and analyze any suspicious network traffic that has been recorded.

Technical Guidance

1. You should be able to obtain the necessary information and downloads from www.netgroup.polito.it to install the forensic software on your forensic PC. The Help menu provides a more detailed documentation of the *Analyzer*.

2. You will need to first unzip the downloaded file before installation.

3. You will be issued a set of ACP files with the network traffic captured on a floppy disk. Open the files in *Analyzer* to perform your analysis.

4. Explore the various functionalities of *Analyzer*. It allows you to describe the protocol format, customize the display of the packets, evaluates statistics, plots graphs, set query on the analysis engine and set filter at the MAC, Network, Transport or Application Layer.

5. Although not required in this exercise, *Analyzer* is also capable of capturing packets from the network for real time monitoring and creating capture files. It uses the *WinPcap* library to capture packets and set monitoring filters on the network traffic monitor.

6. Present your findings in a written report.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1. Barnett, Stephen; 'Computer Security Training And Education: A Needs Analysis', Proceedings of the 1996 IEEE Symposium on Security and Privacy.

2. Casey, Eoghan; Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet,' Academic Press, March 2000.

3. Casey, Eoghan; 'Handbook of Computer Crime Investigation: Forensic Tools & Technology', Academic Press, October 2001.

4. Farmer, Dan; Venemam, Wietse; 'Computer Forensics Column', Doctor Dobb's Journal, www.fish.com/security/ddj.html or www.porcupine.org/forensics.

5. Holley, James; 'Meeting Computer Forensic Analysis Requirements', SC Magazine, March 2001.

6. Irvine, Cynthia; 'Goals for Computer Security Education', Proceedings of the 1996 IEEE Symposium on Security and Privacy, May 1996.

7. Irvine, Cynthia; 'Center For Information Systems Security Studies and Research, NPS Research, June 1998.

8. Irvine, Cynthia; 'Amplifying Security Education in the Laboratory', Proceeding IFIP TC11 WC 11.8 First World Conference on Information Security Education, Kista, Sweden, June 1999.

9. Lang, David; 'Design and Development of a Distance Education Paradigm for Training Computer Forensic Examiners: A Limited Review of Literature', www.computerteacher.org/CFLR.htm, December 1999.

10. Wadlow, Thomas; 'The Process of Network Security: Design and Managing a SafeNetwork', Addison Wesley Longman Inc, February 2000

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Senior Lecturer Daniel F. Warren
   Department of Computer Science
   Naval Postgraduate School
   Monterey, California

4. Profession Dan C. Boger
   Information Systems Academic Group
   Naval Postgraduate School
   Monterey, California